Height Lower Bounds in some non-Abelian Extensions

Inauguraldissertation

zur

Erlangung der Würde eines Doktors der Philosophie

vorgelegt der

Philosophisch-Naturwissenschaftlichen Fakultät

der Universität Basel

von

Linda Karina Frey

aus Deutschland

Basel, 2018

Genehmigt von der Philosophisch-Naturwissenschaftlichen Fakultät auf Antrag von

Prof. Dr. Philipp Habegger

Prof. Dr. Francesco Amoroso

Basel, den 22. Mai 2018

Prof. Dr. Martin Spiess,
Dekan

Contents

1 Acknowledgements

Writing proper acknowledgements seems like an infinitely hard problem. Here is my attempt.

I dedicate this thesis to my husband. His endless love and support made this possible. I thank him for giving me the energy that I needed. Energy - and not time - is the most precious good for parents.

I thank my advisor Philipp Habegger for his most valuable mathematical advice and support. His seemingly infinite mathematical knowledge helped me through many thirst stretches.

I thank Francesco Amoroso for being a very helpful referee and giving constructive comments.

I thank Gabriel Dill for reading my thesis over and over again and always being patient with me.

I thank Fabrizio, Francesco and Gabriel for always providing lovely company and diversion.

I thank Markus, Michalis and Fabian for all the wonderful mathematical and non-mathematical coffee breaks.

I thank the Algebra group, the Number Theory group and my grandmother Anna for having made Basel a second home for me.

I thank Florian Breuer for advice and encouragement

I thank Patricia and Andrea for the antelope program.

I thank all my friends, family and colleages for their support.

I thank my children for always giving me a reason to leave my desk.

I thank my parents for supporting me.

I thank the the University of Basel, the DFG, the University of Darmstadt and

the University of Frankfurt for supporting my research.

I thank Martin Ludwig Michaelis, Martin Zipp, Roland Naumann, Claudia Schütte, Klaus Winkler, Manfred Lehn, Manuel Blickle, Clemens Fuchs, Joachim Rosenthal, Emmanuel Kowalski, Philipp Habegger and many more for nurturing my love of mathematics.

2 Introduction

Kronecker's Theorem states that an algebraic number has *absolute logarithmic Weil height* zero if and only if it is either zero or a root of unity. A natural question to ask is whether we can find an explicit constant $C > 0$ such that the height of any algebraic number is zero or greater or equal to C. The fact that the height of $2^{\frac{1}{n}}$ is $\frac{\log 2}{n}$ shows that the answer is no. If we replace the field of algebraic numbers with a smaller field, there is hope that this is true. We say a field has the *Bogomolov* property if there is a positive constant C such that the height of any non-torsion and non-zero element is greater than C. This property was introduced by Bombieri and Zannier in [BZ01].

By Northcott's Theorem every number field satisfies the Bogomolov property. Although the property was not called Bogomolov yet, in 1973 Schinzel [Sch73] (and later Smyth [Smy81] made the result explicit) proved that $\mathbb{Q}^{\mathrm{tr}}$, the maximal totally real extension of the rational numbers, also satisfies the Bogomolov property. Twenty-seven years later, Amoroso and Dvornicich [AD00] proved that $\mathbb{Q}^{\mathrm{ab}}$, the maximal abelian extension of the rationals, satisfies the Bogomolov property and they even found an explicit lower bound, namely $\frac{\log 5}{12}$. This bound is almost sharp (there is an element of height $\frac{\log 7}{12}$). By the Theorem of Kronecker-Weber, the field $\mathbb{Q}^{\mathrm{ab}}$ can be obtained by adjoining μ_∞, the set of all roots of unity, to the rationals. In 2000 and 2010, Amoroso and Zannier ([AZ00] effective and [AZ10] uniform and explicit) in a similar setting proved the following: Let $\alpha \in \overline{\mathbb{Q}}^* \setminus \mu_\infty$ such that there exists a number field K of degree d over $\mathbb{Q}$ with $K(\alpha)/K$ abelian. Then $h(\alpha) \geq 3^{-d^2-2d-6}$. A survey article by Smyth on that topic [Smy08] which cites 173 articles shows that this topic is still of great interest.

Another remarkable paper is [ADZ14], where one can find a good overview of the Bogomolov property. The authors prove that any Galois extension L of a number field K such that $G/Z(G)$ has finite exponent, where G is the galois group of L/K and $Z(G)$ is its center, is Bogomolov. We use the idea of the proof of their Lemma 2.1 in our Section 4.2.2. Furthermore, their result seems similar to one of our results where we consider an infinite extension of such a field.

Now we turn to elliptic curves and create the elliptic curve analogue to $\mathbb{Q}^{\mathrm{ab}}$. Let E be an elliptic curve defined over $\mathbb{Q}$ and let $\mathbb{Q}(E_{\mathrm{tor}})$ be the smallest field extension of $\mathbb{Q}$ that contains all coordinates of torsion points of E. In 2013 Habegger [Hab13] showed that $\mathbb{Q}(E_{\mathrm{tor}})$ satisfies the Bogomolov property. The aim of this paper is

making this result explicit (not only effective!). Whenever an elliptic curve admits some endomorphism over $\overline{\mathbb{Q}}$ that is not multiplication by an integer, we say the elliptic curve has complex multiplication or short is CM. In the CM case, $\mathbb{Q}(E_{\mathrm{tor}})$ has the Bogomolov property by the result of Amoroso and Zannier [AZ00] and this becomes explicit using their later work [AZ10]. So we can concentrate on the other case: For a non-CM elliptic curve, this extension is non-abelian and none of the above results can be applied.

We will now explain the structure of this thesis. Chapter 2 shortly introduces some number theory to the reader. In Chapter 3 and 4 we will state and prove the main theorems. Chapter 3 is about making Habegger's result explicit and chapter 4 generalizes it. The first main theorem of chapter 3 is the following.

Theorem 2.1
Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multilplication and let $p \geq 5$ be a supersingular prime of E such that the Galois representation $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\, E[p]$ is surjective. Then for all $\alpha \in \mathbb{Q}(E_{tor})^* \setminus \mu_\infty$ we have

$$h(\alpha) \geq \frac{(\log p)^5}{10^{21} p^{44}}.$$

By Elkies [Elk89] and Serre [Ser72], such a prime always exists. After bounding the smallest supersingular and surjective prime p, we get the following theorem.

Theorem 2.2
Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. Let $\alpha \in \mathbb{Q}(E_{tor})^* \setminus \mu_\infty$. Then with $n = 10^7 \max\{985, \frac{1}{12}(18N \log N) + 3\}^2$ we have

$$h(\alpha) \geq ((8Ne^{\vartheta(n)})^{Ne^{\vartheta(n)}(\log(8Ne^{\vartheta(n)}))^5} 18N \log N)^{-44}$$

where $\vartheta(n) = \sum_{p \leq n} \log p$.

In chapter 4, we will generalize Habegger's result and allow larger base fields as follows.

Theorem 2.3
Let E be an elliptic curve over $\mathbb{Q}$. Let L be a (possibly infinite) Galois extension of $\mathbb{Q}$ with uniformly bounded local degrees by $d \in \mathbb{N}$. Then $L(E_{tor})$ satisfies the Bogomolov property.

Given a prime p such that p is surjective, supersingular and greater than $\max(2d+2, \exp(\mathrm{Gal}(L/\mathbb{Q}))$ (which is always finite by [Che13]), we can even explicitly compute the lower bound for the height and it is $\frac{(\log p)^4}{p^5 p^3}$.

We now want to sketch the proofs.

We start with the explicit result. We will dive into Habegger's paper where two parts are important for us. First, he proves that the height of an element $\alpha \in \mathbb{Q}(E_{\text{tor}})^* \setminus \mu_\infty$ plus a correction term is bounded from below. There the bound depends on a prime p that fulfills the conditions of the above Theorem 2.1. To be more precise, he proves the following.

Proposition 2.4 ([Hab13], Proposition 6.1)
Suppose E does not have complex multiplication. There exists a constant $c > 0$ depending only on E with the following property. If $\alpha \in \mathbb{Q}(E_{tor}) \setminus \mu_\infty$ is non-zero, there is a non-zero $\beta \in \overline{\mathbb{Q}} \setminus \mu_\infty$ with $h(\beta) \leq c^{-1}h(\alpha)$ and

$$h(\alpha) + \max\{0, \frac{1}{[\mathbb{Q}(\beta) : \mathbb{Q}]} \sum_{\tau:\mathbb{Q}(\beta)\to\mathbb{C}} \log|\tau(\beta) - 1|\} \geq c.$$

Second, he uses Bilu's equidistribution Theorem in [Bil97] with a modification of the logarithmic term to avoid the logarithmic singularity.

We will follow this structure and first bound the prime p in Section 4.1. Here we have to find a small supersingular prime. Although Fouvry and Ram Murty [FRM96] prove a lower bound for the number of supersingular primes less than or equal to x, their bound is not explicit in terms of E so we have to find such a bound. We will do so by following Elkies' constructive proof [Elk89] of the existence of infinitely many supersingular primes for an elliptic curve and make it explicit. We will get some congruence relations and put them into one single congruence relation. This allows us to find supersingular primes by finding primes in an arithmetic progression. An unpublished result of Bennett, Martin, O'Bryant and Rechnitzer [BMOR18] then gives us an explicit bound for that prime. We will also give an effective version where we use Linnik's theorem [Xyl11a], but unfortunately the estimates in this references are not explicit, . Furthermore, we have to give a bound for the biggest non-surjective prime. For that we will quote a result of Le Fourn, [LF16].

Next, we will get rid of the sum in Proposition 3.13. Instead of modifying the logarithmic term as in [Hab13] and applying an effective version of Bilu's Theorem, we provide a direct route via a height bound for polynomials due to Mignotte [Mig89], see Section 4.2.1.

In Section 4.4 we will give some examples of elliptic curves and their corresponding explicit height bounds.

Since this height bound depends on the elliptic curve via the prime p, it makes sense searching for a prime p that is supersingular and surjective for an infinite family of elliptic curves. That would give an unconditional explicit lower bound for the whole family. But while the supersingularity condition can probably be expressed by finitely many congruence relations, finding an unconditional bound for surjective

primes is related to an open conjecture of Serre. A possibility may also be looking only at semistable curves and finding an infinite family of semistable curves with the techniques of Kramer [Kra83].

The proof of our Theorem 2.3 involves the theory of local fields, ramification theory and Galois theory. In his proof, Habegger makes heavy use of the Frobenius. In our generalized case, we can not always be sure that there exists a lift of the Frobenius. We will work around that by taking suitable powers of suitable morphisms. Another key ingredient in Habegger's proof are non-split Cartan subgroups. In our proof we can completely work around that by considering the unramified and the tamely ramified case together.

There is also the complementary problem where we do not look at an extension of $\mathbb{Q}$ but at the Néron-Tate height of the elliptic curve E itself. Recall that the Néron-Tate height vanishes precisely at the points of finite order of E. Baker [Bak03] proved that for an elliptic curve E either having complex multiplication or non-integral j-invariant, the Néron-Tate height on $E(\mathbb{Q}^{\mathrm{ab}}) \setminus E_{\mathrm{tor}}$ is bounded from below. Silverman [Sil04] proved the same without the constraint on E. There are two generalizations of this. First, Baker and Silverman [BS04] proved the existence of a lower bound for $A(\mathbb{Q}^{\mathrm{ab}}) \setminus A_{\mathrm{tor}}$ where A is an abelian variety. Second, Habegger [Hab13] proved that the Néron-Tate height on $E(\mathbb{Q}(E_{\mathrm{tor}})) \setminus E_{\mathrm{tor}}$ is bounded from below. The general conjecture is the following.

Conjecture 2.5 (David)
Let A be an abelian variety defined over a number field K equipped with a Néron-Tate height coming from a symmetric and ample line bundle. Then the Néron-Tate height on $A(K(A_{tor})) \setminus A_{tor}$ is bounded from below by a constant only depending on A/K and the definition of the height.

A future task can be making Habegger's bound on the Néron-Tate height explicit.

3 Preliminaries

3.1 Notations

$\mathbb{Q}$	field of rational numbers
$\mathbb{Z}$	ring of rational integers
$\mathbb{H}$	the upper half plane $\{z \in \mathbb{C} \mid \operatorname{im} z > 0\}$
h_ℓ	the class number of $\mathbb{Q}(\sqrt{-\ell})$
$\operatorname{rad}(a)$	product of the distinct prime divisors of an integer $a \neq 0$
$\varphi(a)$	number of invertible residues modulo a
μ_∞	set of all roots of unity
μ_n	set of roots of unity of order dividing n
$\pi(a)$	number of primes less than or equal to a
p	prime number
$\vartheta(a)$	$\sum_{p \leq a} \log p$
K_v	completion of a field K with respect to a place v
$\operatorname{Num}(x)$	numerator of a rational number x
$\operatorname{Denom}(x)$	denominator of a rational number x
$\mathbb{Q}_p$	field of p-adic numbers
$\mathrm{E}_{\mathrm{tor}}$	torsion points of an elliptic curve E
$E[N]$	N-torsion points of an elliptic curve E
$\lvert \cdot \rvert_v$	v-adic absolut value
$h(x)$	absolute logarithmic Weil height of x
$h^*(x)$	positive absolute logarithmic Weil height of x, $h^*(x) = \max(\log 2, h(x))$
$K(N)$	$K(N) = K(E[N])$ where $E[N]$ are the N-torsion points of an elliptic curve E defined ov
$e(K : L)$	ramification index of K over L
$\exp(G)$	exponent of a group G
$\mathbb{Q}_q$	the unique quadratic unramified extension of $\mathbb{Q}_p$

3.2 Elliptic curves

In this chapter we will give the basic definitions in the theory of elliptic curves. Since the results in this section are basic and available in all standard books we will skip the proofs and refer to [Sil09] for deeper interest. We will also closely follow Silverman's notations and definitions.

Definition 3.1 (Elliptic curve)
An elliptic curve E over a field K is given by the equation $Y^2 = X^3 + AX + B$ with $A, B \in K$ and $4A^3 + 27B^2$ is non-zero. Then for any field L containing K we set $E(L) := \{(x, y) \in L^2 | y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$ where $\mathcal{O}$ is the point at infinity. There is a well-known group structure on E where two distinct points are added by taking the third intersection point of the line through the points and the elliptic curve and mirroring it on the x-axis. One can add a point to itself by taking the tangent line instead of the line through two distinct points. For $N \in \mathbb{N}$ we call $E(L)[N] := \{(x, y) \in E(L) | N \cdot (x, y) = \mathcal{O}\}$ the N-torsion points and $E_{\text{tor}} := \bigcup_{N \in \mathbb{N}} E(\overline{\mathbb{Q}})[N]$ the torsion points.

Remark 3.2
One can also define an elliptic curve as a smooth projective algebraic curve of genus one with a specified point $\mathcal{O}$. But since we care for explicit coordinates, the above definition suits our case better.

Definition 3.3 (Conductor, j-invariant)
We call $j_E := \frac{4A^3}{4A^3+27B^2}$ the j-invariant of E. For the precise definition of the conductor N of an elliptic curve E, we refer to §10 in [Sil94]. For us, the following facts will be sufficient:

- $\frac{\text{rad}(6N)}{6}$ is the product of all primes $p \geq 5$ such that the reduction of E mod p is a singular curve.
- For elliptic curves over $\mathbb{Q}$, the conductor is always at least 11 (see [Cre97], Table 1) .

Definition 3.4 (Complex multiplication)
Let E be an elliptic curve over $\mathbb{Q}$. We call $\text{End}(E)$ the set of $\overline{\mathbb{Q}}$-endmorphisms of E. Since we can add points to themselves, it will always contain $\mathbb{Z}$. In the case where $\text{End}(E)$ is strictly larger than $\mathbb{Z}$, we say that E *has complex multiplication.* If a ring R can be embedded in $\text{End}(E)$, we say that E *has complex multiplication by* R.

Remark 3.5
For an elliptic curve over $\mathbb{Q}$, the following is true. Whenever $\text{Aut}(E)$ is strictly larger than $\mathbb{Z}$, it will be of the form $\mathcal{O}_D = \mathbb{Z}[\frac{1}{2}(D + \sqrt{D})]$ for D congruent to 0 or 3 modulo 4. In that case we say that E has *complex multiplication by* $\mathcal{O}_D$.

Definition 3.6 (Supersingular prime)
Let E be an elliptic curve over $\mathbb{Q}$ and let $p \in \mathbb{Z}$ be a prime. We say that p is *supersingular* for E if the reduction E_p of E mod p is a non-singular curve and has complex multiplication by some $\mathcal{O}_D$ such that p is ramified or inert in $\mathbb{Q}(\sqrt{-D})$.

Elkies' result tells us that there are many of them.

Theorem 3.7 (Elkies, [Elk87])
Let E be an elliptic curve over $\mathbb{Q}$. Then there are infinitely many supersingular primes for E.

In [FRM96] Fouvry and Ram Murty proved that the number of supersingular primes for an elliptic curve E that are smaller than a sufficiently large x is at least $c \log\log x$ for an absolute positive constant c but this result is not explicit.

Definition 3.8 (Surjective primes)
Let E be an elliptic curve defined over $\mathbb{Q}$ and let $p \in \mathbb{N}$ be a prime. We say that p is *surjective* (for E) if the Galois representation $\rho_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\ E[p]$ is surjective.

Serre's Théorème in [Ser72] states that there is a bound such that all primes greater than that bound are surjective if E does not have complex multiplication. Originally, his result contained no explicit bound. Explicit and effective estimates for this bound were developed later. One example is the following result of Le Fourn which we will state in the section on heights.

The proof of Elkies' Theorem gives an algorithm for finding supersingular primes. It requires finding primes in arithmetic progressions. Dirichlet's Theorem tells us that we can find such a prime and Linnik's Theorem tells us how big it is. Although many authors have improved the exponent in Linnik's Theorem not much has appeared in the literature on the multiplicative constant and only effective, but not explicit results are known there. Bennett, Martin, O'Bryant and Rechnitzer equip us with another result which is asymptotically weaker than Linnik's Theorem and its refinements but which is completely explicit.

We want to introduce two properties that we need later on.

Definition 3.9
Let $p \geq 5$ and let E be an elliptic curve over $\mathbb{Q}$. We say that p has property (P1) if p is a supersingular prime for E. We say that p has property (P2) if p is surjective.

3.3 Local Fields

We want to introduce some basic ramification theory and use the definitions of Neukirch [Neu99].

Definition 3.10 (Ramification index and inertia degree)
Let K be a number field and L be a finite Galois extension of K. Let v be a finite place of K and w be a finite place of L that extends v. The index

$$e = e(w|v) = (w(L^*) : v(K^*))$$

is called the *ramification index* of the extension L/K. We call L *totally ramified (at w)* if $e = [L : K]$ and *unramified (at w)* if $e = 1$.

Definition 3.11 (Higher ramification group)
Let now L/K be a finite extension of local fields with $w : L \to \mathbb{Z} \cup \{+\infty\}$ the surjective valuation and for $i \geq -1$ we call

$$G_i(L/K) := \{\sigma \in \mathrm{Gal}(L/K) | \forall a \in \mathcal{O}_K \text{ we have } w(\sigma(a) - a) \geq i + 1\}$$

the *i-th higher ramification group of L/K*.

Remark that G_{-1} is the Galois group and G_0 is the inertia group. By definition 10.1 of [Neu99], we have

$$G_{-1}(L/K) \supset G_0(L/K) \supset G_1(L/K) \supset ...$$

and the G_i are normal subgroups of $G_{-1}(L/K)$.

3.4 Heights

Definition 3.12 (Height)
Let $x \in \overline{\mathbb{Q}}$ and let K be any number field that contains x. Then we define the *(absolute logarithmic Weil) height* of x as

$$h(x) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log(\max(|x|_v, 1))$$

where M_K is the set of places of K, $d_v = [K_v : \mathbb{Q}_p]$ are the local field degrees and the absolute values are normalized such that $|p|_p = \frac{1}{p}$. Later on we will also need the following notation: $h^*(x) := \max(\log 2, h(x))$.

This definition is independent of the choice of K. The definition of h^* guarantees that we always have $h(x) \leq h^*(x)$ and $h^*(x)$ is always positive.

The main ingredient in our recipe is:

Proposition 3.13 (Habegger, Proposition 6.1, [Hab13])
Suppose E does not have complex multiplication. Let $p \geq 5$ be a surjective and supersingular prime for E. If $\alpha \in \mathbb{Q}(E_{tor})^* \setminus \mu_\infty$ then there is a $\beta \in \overline{\mathbb{Q}^*} \setminus \mu_\infty$ with $h(\beta) \leq 10p^4 h(\alpha)$ and

$$h(\alpha) \geq \frac{1}{5}\left(\frac{\log p}{2p^8} - \max\Big\{0, \frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]} \sum_{\tau:\mathbb{Q}(\beta)\hookrightarrow\mathbb{C}} \log|\tau(\beta) - 1|\Big\}\right).$$

In the section about the small heights, we want to compare the height of an algebraic number with its degree and two theorems of Voutier can help us with that.

Theorem 3.14 (Voutier, [Vou96], main theorem)
Let $\alpha \in \overline{\mathbb{Q}^*} \setminus \mu_\infty$ with $d := \deg \alpha \geq 2$ then we have

$$h(\alpha) > \frac{1}{4d}\left(\frac{\log\log d}{\log d}\right)^3.$$

With Corollary 2 of the same paper we get

Corollary 3.15 (Voutier, [Vou96], Corollary 2)
Let $\alpha \in \overline{\mathbb{Q}^*} \setminus \mu_\infty$ with $d := \deg \alpha \leq 16$ then we have

$$h(\alpha) \geq \frac{1}{8(\log 48)^3}.$$

Now we can also state the aforementioned bound for supersingular primes of Le Fourn:

Theorem 3.16 ([LF16], Theorem 4.2)
Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and let j_E be the j-invariant of E. Then for

$$p > 10^7 \max\{985, \frac{1}{12}h(j_E) + 3\}^2$$

the Galois representation ρ_p is surjective.

4 The explicit height bound

4.1 A supersingular prime for E

Let E be an elliptic curve over $\mathbb{Q}$. We let N be the conductor and j_E be the j-invariant of E. We want to find a small supersingular prime for E. In his paper Elkies [Elk87] demonstrated how to find such a prime. We will use this technique to find a supersingular prime which we can bound explicitly in terms of constants depending only on E. Fouvry and Murty [FRM96] prove a lower bound for the number of supersingular primes less than or equal to x. Yet the dependency on E in their bound is not made explicit.

For now we consider primes $\ell \equiv 3 \bmod 4$ and let h_ℓ be the class number of $\mathbb{Q}(\sqrt{-\ell})$. For positive D such that $-D$ is the discriminant of $\mathbb{Z}[\frac{D+\sqrt{-D}}{2}]$ let P_D be the monic polynomial whose roots are (with multiplicity one) exactly the finitely many j-invariants of non-isomorphic elliptic curves with complex multiplication by $\mathbb{Z}[\frac{D+\sqrt{-D}}{2}]$. They are polynomials with coefficients in $\mathbb{Z}$ (see [Elk87]). We introduce the convention $\sqrt{-\ell} = i\sqrt{\ell}$ where $\sqrt{\ell}$ is the positive root of ℓ.

We start with a definition.

Definition 4.1 (Modular j-function)
Let $\tau \in \mathbb{H}$ and let $q = e^{2\pi i \tau}$. We define

$$\Delta(\tau) = g_2(\tau)^3 - 27 g_3(\tau)^2,$$

where

$$g_2(\tau) = (2\pi)^4 \frac{1}{2^2 \cdot 3}(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n)$$

and

$$g_3(\tau) = (2\pi)^6 \frac{1}{2^3 \cdot 3^3}(1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n)$$

with $\sigma_k(n) = \sum_{d|n} d^k$. Then we call

$$j(\tau) = 1728 \frac{g_2(\tau)^3}{\Delta(\tau)}$$

the *modular j-function.*

As Elkies describes in [Elk87], $j(\frac{1+\sqrt{-\ell}}{2})$ and $j(\sqrt{-\ell})$ are the only real roots of P_ℓ and $P_{4\ell}$, respectively. So both P_ℓ and $P_{4\ell}$ must have odd degree since they have only one real root and all other roots have to fall into pairs of complex conjugate numbers. Also, we constructed the polynomials to be monic. For the next lemma we cite a paragraph in [Elk87]:

Remark 4.2 ([Elk87], end of chapter 2)
From the q-expansion: $j(z) = \exp(-2\pi iz)+O(1)$ as $\operatorname{im} z \to \infty$, we see that these real roots go to $-\infty$ (for P_ℓ) and $+\infty$ (for $P_{4\ell}$) as ℓ increases. Thus for fixed $J, P_\ell(J) > 0$ and $P_{4\ell} < 0$ for ℓ sufficiently large.

We now want to find a lower bound B_E such that given an elliptic curve with j-invariant j_E, for all $\ell \geq B_E$ we have $P_\ell(j_E) > 0$ and $P_{4\ell}(j_E) < 0$.

Lemma 4.3
Let E be an elliptic curve over $\mathbb{Q}$ with j-invariant j_E, let

$$B_E = \begin{cases} \left(\frac{\log j_E}{2\pi}\right)^2 & \text{if } j_E > 0, \\ \left(\frac{\log |j_E|}{\pi} + 1\right)^2 & \text{if } j_E < 0, \\ 0 & \text{if } j_E = 0. \end{cases}$$

Then for all primes $\ell > \max\{B_E, 7\}$ such that $\ell \equiv 3 \bmod 4$ we have $j(\frac{1+\sqrt{-\ell}}{2}) < j_E < j(\sqrt{-\ell})$, hence $P_\ell(j_E) > 0$ and $P_{4\ell}(j_E) < 0$.

Proof
By the discussion on the real roots of P_ℓ and $P_{4\ell}$, we see that $j(\frac{1+\sqrt{-\ell}}{2}) < j_E < j(\sqrt{-\ell})$ implies $P_\ell(j_E) > 0$ and $P_{4\ell}(j_E) < 0$. By [Lan73], Theorem 5 on page 249, we have $\Delta(\tau) = (2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24}$ with $q = e^{2\pi i\tau}$.

Let now $\tau = \sqrt{-\ell}$, so $q = e^{2\pi i\sqrt{-\ell}} = e^{-2\pi\sqrt{\ell}}$ with ℓ a prime number. Since $\prod_{n=1}^{\infty}(1-q^n)^{-24} = \prod_{n=1}^{\infty}\left(\sum_{k=0}^{\infty} q^{nk}\right)^{24}$ is a product of geometric series with positive coefficients, it has positive coefficients as a series in q and we get $1728 g_2(\tau)^3\Delta(\tau)^{-1} = \frac{1}{q}\sum_{i=0}^{\infty} a_i q^i$ with positive integers a_i and $a_0 = 1$. So we get

$$j(\sqrt{-\ell}) = 1728 g_2(\tau)^3\Delta(\tau)^{-1} > \frac{1}{q} = e^{2\pi\sqrt{\ell}}. \tag{4.1}$$

Let now $\tau = \frac{1+\sqrt{-\ell}}{2}$, again with ℓ a prime number, so $q = e^{2\pi i\frac{1+\sqrt{-\ell}}{2}} = -e^{-\pi\sqrt{\ell}}$.

For $\ell \geq 7$ we have

$$\begin{aligned}\log\left(\prod_{n=1}^{\infty}(1-q^n)^{-24}\right) &\geq -24\sum_{n=1}^{\infty}\log(1+|q|^n)\\ &\geq -24\sum_{n=1}^{\infty}|q|^n\\ &= -24\frac{|q|}{1-|q|}\\ &> \log(0.99).\end{aligned}$$

Furthermore, by [Lan73], proposition 4 on page 47, we have

$$g_2(\tau) = \frac{(2\pi)^4}{12}(1+240\sum_{n=1}^{\infty}n^3\frac{q^n}{1-q^n})$$

. Now we want to bound $\frac{q^n}{1-q^n}$. Consider first the case where n is odd (hence $q^n \leq 0$). Since $\ell \geq 7$ we get $\frac{q^n}{1-q^n} = \frac{-|q|^n}{1+|q|^n} \geq \frac{q^n}{1+e^{-\pi\sqrt{7}}} \geq \frac{q^n}{1.0003}$. In the case where n is even (hence $q^n \geq 0$), we even get $\frac{q^n}{1-q^n} \geq q^n$. This gives

$$\begin{aligned}\frac{12}{(2\pi)^4}g_2(\tau) &= 1+240\sum_{n=1}^{\infty}n^3\frac{q^n}{1-q^n}\\ &\geq 1+239\sum_{n=1}^{\infty}n^3q^n\\ &= 1+239q\frac{1+4q+q^2}{(1-q)^4}\\ &\geq 0.94.\end{aligned}$$

We put both inequalities together and get

$$j(\frac{1+\sqrt{-\ell}}{2}) = \frac{1}{q}(\frac{12}{(2\pi)^4}g_2(\tau))^3\prod_{n=1}^{\infty}(1-q^n)^{-24} \leq \frac{1}{q}0.94^3\cdot 0.99 \leq -0.82\cdot e^{\pi\sqrt{\ell}}. \tag{4.2}$$

So for $\tau = \sqrt{-\ell}$ (and hence q positive) we get

$$0 < e^{2\pi\sqrt{\ell}} = \frac{1}{q} < j(\sqrt{-\ell}) \tag{4.3}$$

and for $\tau = \frac{1+\sqrt{-\ell}}{2}$ (and hence q negative) we get

$$j(\frac{1+\sqrt{-\ell}}{2}) \leq 0.82\frac{1}{q} = -0.82\cdot e^{\pi\sqrt{\ell}} < 0. \tag{4.4}$$

For $j_E \geq 0$ the inequality $j(\frac{1+\sqrt{-\ell}}{2}) < j_E$ holds true by equation (4.4) and for $j_E \leq 0$ the inequality $j_E < j(\sqrt{-\ell})$ holds true by equation (4.3). So we can take $B_E = 0$ if $j_E = 0$. Moreover, to complete the proof we may assume $j_E \neq 0$ and it suffices to show:

$$j_E < e^{2\pi\sqrt{\ell}} \text{ if } j_E > 0$$

and

$$j_E > -0.82 \cdot e^{\pi\sqrt{\ell}} \text{ if } j_E < 0.$$

The first inequality follows from

$$\left(\frac{\log j_E}{2\pi}\right)^2 < \ell$$

and the second one from

$$\left(\frac{\log |j_E|}{\pi} - \frac{\log 0.82}{\pi}\right)^2 < \ell$$

and we proved the statement. □

By Elkies ([Elk87]), we know that we can find a supersingular prime for E by taking a prime ℓ such that $\left(\frac{-1}{\ell}\right) = -1$ and $\left(\frac{p}{\ell}\right) = +1$ for every prime p of bad reduction. Since j_E is a rational number, $P_\ell(j_E)P_{4\ell}(j_E)$ is also rational and it makes sense to speak of numerators and denominators. Then the factorization of the numerator of either $P_\ell(j_E)$ or $P_{4\ell}(j_E)$ contains a supersingular prime for E. So if we can find such an ℓ and bound the numerator of $P_\ell(j_E)P_{4\ell}(j_E)$, we also get a bound for a supersingular prime for E.

We start by bounding $\mathrm{Num}(P_\ell(j_E)P_{4\ell}(j_E))$.

Lemma 4.4 (Fouvry-Ram Murty, [FRM96], Lemma 5)
With the notation from before and $C = 10^4 \log(|j_E| + 745)$ *we have*

$$|P_\ell(j_E)P_{4\ell}(j_E)| \leq e^{2C\sqrt{\ell}(\log \ell)^2 + 4h_\ell}.$$

Proof
For an integer $a \neq 0$, let $v(a)$ be the number of its distinct prime divisors. We use the following inequalities from [RM88]:

$$|P_\ell(j_E)| \leq 2^{h_\ell} e^{\log(|j_E|+745)\sqrt{\ell}\sum_{1\leq a\leq\sqrt{\ell}} \frac{2^{v(a)}}{a}} \text{ (Lemma 5)}$$

and

$$|P_{4\ell}(j_E)| \leq^{[F:\mathbb{Q}_q]} 3h_\ell e^{4\log(|j_E|+745)\sqrt{\ell}\sum_{1\leq a\leq\sqrt{\ell}} \frac{2^{v(a)}}{a}} \text{ (Lemma 6)}.$$

Now we follow the proof of Fouvry and Ram Murty:

$$\begin{aligned}\sum_{1\le a\le\sqrt{\ell}}\frac{2^{v(a)}}{a} &\le \prod_{p\le\sqrt{\ell}}\left(1+\frac{2}{p}+\frac{2}{p^2}+\frac{2}{p^3}+...\right) \text{ (where the product is over all primes up to } \sqrt{\ell})\\ &= \prod_{p\le\sqrt{\ell}}\left(1+\frac{2}{p}\sum_{k=0}^{\infty}\frac{1}{p^k}\right)\\ &= \prod_{p\le\sqrt{\ell}}\left(1+\frac{2}{p-1}\right).\end{aligned}$$

Now we take the logarithm.

$$\begin{aligned}\log\prod_{p\le\sqrt{\ell}}\left(1+\frac{2}{p-1}\right) &\le \sum_{p\le\sqrt{\ell}}\frac{2}{p-1}\\ &= 2\sum_{p\le\sqrt{\ell}}\left(\frac{1}{p}+\frac{1}{(p-1)p}\right)\\ &\le 2\sum_{p\le\sqrt{\ell}}\left(\frac{1}{p}+\frac{2}{p^2}\right) && \text{since } \frac{p}{2}\le p-1\\ &\le 2\sum_{p\le\sqrt{\ell}}\frac{1}{p}+4\sum_{n=1}^{\infty}\frac{1}{n^2}\\ &\le 2\log\log\sqrt{\ell}+0.523+\frac{2}{(\log\sqrt{\ell})^2}+2\frac{\pi^2}{3} && \text{see [RS62], Cor after Thm 5.}\end{aligned}$$

So we get

$$\begin{aligned}\sum_{1\le a\le\sqrt{\ell}}\frac{2^{v(a)}}{a} &\le \frac{1}{4}e^{0.523+\frac{2}{(\log\sqrt{7})^2}+2\frac{\pi^2}{3}}(\log\ell)^2\\ &\le 2513(\log\ell)^2\\ &\le 2.6\cdot 10^3(\log\ell)^2.\end{aligned}$$

And as a result

$$\begin{aligned}|P_\ell(j_E)P_{4\ell}(j_E)| &\le 2^{h_\ell}e^{2.6\cdot 10^3\log(|j_E|+745)\sqrt{\ell}(\log\ell)^2}2^{3h_\ell}e^{1.1\cdot 10^4\log(|j_E|+745)\sqrt{\ell}(\log\ell)^2}\\ &\le e^{2C\sqrt{\ell}(\log\ell)^2+4\log(2)h_\ell}.\end{aligned}$$

□

Lemma 4.5
With the notation of the lemma before, $\ell\equiv 3$ mod 4 and $\ell\ge 5$ we have

$$|\operatorname{Num}(P_\ell(j_E)P_{4\ell}(j_E))| \le e^{2\cdot 10^5\sqrt{\ell}(\log\ell)^2h^*(j_E)}.$$

Proof
By [Sil94], App C, Prop. 11.1, we know $\deg P_\ell = h_\ell$ and by [Coh80], p. 217 thm 2, we have $\deg P_\ell = \deg P_{4\ell}$.

Furthermore, by [Hua82], Theorem 10.1 (page 323) and Theorem 14.3 inequality (3) (page 330), and since $\ell \geq 7$ we can use the class number formula to get the following bound:

$$h_\ell \leq \frac{2\sqrt{\ell}}{2\pi}(2 + \log \ell) \leq \frac{7\sqrt{\ell}\log \ell}{2\pi}.$$

So

$$\deg(P_\ell P_{4\ell}) = 2h_\ell \leq \frac{7\sqrt{\ell}\log \ell}{\pi}$$

and using Lemma 4.4 we get:

$$|P_\ell(j_E)P_{4\ell}(j_E)| \leq e^{2C\sqrt{\ell}(\log \ell)^2 + 4h_\ell} \leq e^{2C\sqrt{\ell}(\log \ell)^2 + \frac{14\sqrt{\ell}\log \ell}{\pi}}.$$

Now we can bound the numerator of $P_\ell(j_E)P_{4\ell}(j_E)$.

With $h^*(j_E) \geq \log 2 > 0$ and $\log(\mathrm{Denom}(j_E)) \leq h^*(j_E)$ we get

$$\begin{aligned}
|\operatorname{Num}(P_\ell(j_E)P_{4\ell}(j_E))| &\leq e^{3C\sqrt{\ell}(\log \ell)^2 + \frac{14\sqrt{\ell}\log \ell}{3\pi}} |\operatorname{Denom}(j_E)|^{\frac{7\sqrt{\ell}\log \ell}{\pi}} \\
&= e^{2C\sqrt{\ell}(\log \ell)^2 + \frac{14\sqrt{\ell}\log \ell}{\pi} + \frac{7\sqrt{\ell}\log \ell}{\pi}\log|\operatorname{Denom}(j_E)|} \\
&\leq e^{2C\sqrt{\ell}(\log \ell)^2 + \frac{14\sqrt{\ell}\log \ell}{\pi} + \frac{7\sqrt{\ell}\log \ell}{\pi}h^*(j_E)} \\
&\leq e^{\sqrt{\ell}(\log \ell)^2(2C + 4.5 + 2.3h^*(j_E))} \\
&= e^{\sqrt{\ell}(\log \ell)^2(2\cdot 10^4 \log(|j_E|+745) + 4.5 + 2.3h^*(j_E))} \\
&= e^{\sqrt{\ell}(\log \ell)^2(2\cdot 10^4 \log 745 \log(|j_E|) + 4.5 + 2.3h^*(j_E))} \\
&= e^{\sqrt{\ell}(\log \ell)^2(2\cdot 10^4 \log 745 h^*(j_E) + 4.5 + 2.3h^*(j_E))} \\
&= e^{\sqrt{\ell}(\log \ell)^2 2\cdot 10^5 h^*(j_E)},
\end{aligned}$$

which is what we wanted to show. □

Now we can use the following explicit bound for primes in arithmetic progressions to bound ℓ and hence get an estimate for p:

Theorem 4.6 (Theorem 1.2, [BMOR18])
Let $q \geq 3$ and $\gcd(a, q) = 1$. There exist explicit positive constants $c_\theta(q)$ and $x_\theta(q)$ such that

$$|\theta(x; q, a) - \frac{x}{\varphi(q)}| < c_\theta(q)\frac{x}{\log x} \text{ for all } x \geq x_\theta(q)$$

where $\theta(x;q,a) = \sum_{p \leq x, p \equiv a \bmod q} \log p$ *and* φ *is Euler's* φ*-function. Moreover,*

$$c_\theta \leq \frac{1}{180},$$

while $x_\theta(q)$ *satisfies* $x_\theta(q) < x_0(q)$ *where*

$$x_0(q) = \begin{cases} 4.1 \cdot 10^9, & \text{if } 3 \leq q \leq 16 \\ 6.7 \cdot \frac{10^{10}}{q}, & \text{if } 17 \leq q \leq 10^5 \\ \exp(0.03\sqrt{q}(\log q)^3), & \text{if } q > 10^5 \end{cases}. \tag{4.5}$$

We can derive the following corollary.

Corollary 4.7
Let $q > 10^5$ *and* a *be coprime positive integers. Then there exists a prime* $p \equiv a \bmod q$ *with* $p \leq \exp(\frac{q}{180})$.

Proof
Assume $\theta(x;q,q) = 0$. For $x = \exp(\frac{q}{180})$ we have

$$\begin{aligned} |\theta(x;q,a) - \frac{x}{\varphi(q)}| &= \frac{x}{\varphi(q)} \\ &< c_\theta \frac{x}{\log x} \\ &< \frac{x}{180 \log x} \end{aligned}$$

which is equivalent to $180 \log x < \varphi(q)$. Since $x = \exp(\frac{q}{180})$, this gives $q < \varphi(q)$ which is a contradiction. Hence $\theta(x;q,a)$ cannot be zero and there must be a prime less than $\exp(\frac{q}{180})$. □

Now we can turn to our theorem.

Theorem 4.8
Let E *be an elliptic curve with* j*-invariant* j_E *and conductor* N*. Let* B_E *be as in Lemma 4.3,* $M \in \mathbb{N}$ *and* $n = \max(11, M, B_E)$*. Then there exists a supersingular prime* p *of* E *such that* $p \geq n$ *and*

$$\log p \leq 4 \cdot 10^3 e^{\frac{1}{300} N e^{\vartheta(n)}} (N e^{\vartheta(n)})^2 h^*(j_E).$$

Remark 4.9
We put the artificial condition of p being larger than a given $M \in \mathbb{N}$ in order to be able to make p have certain properties. Later on, we will need p to be surjective and by assuring that it is large enough we can make that happen.

Proof
In this proof we will follow Elkies' construction of supersingular primes in his paper [Elk87].

Let us assume as usual that $\ell \equiv 3 \bmod 4$ (hence $\ell \geq 7$). By the proposition in the said paper, we know that the product $P_\ell P_{4\ell}$ is a square modulo ℓ. Since P_ℓ and $P_{4\ell}$ are monic, also their product $P_\ell P_{4\ell}$ is monic. Since both polynomials are of the same degree and the denominator of $(P_\ell P_{4\ell})(j_E)$ is the denominator of j_E, the nominator of $(P_\ell P_{4\ell})(j_E)$ also has to be a square modulo ℓ. We already proved that for every $\ell > \max(B_E, 7)$ as in Lemma 4.3, the numerator of $P_\ell(j_E)P_{4\ell}(j_E)$ is a negative integer, that is $\mathrm{Num}(P_\ell(j_E)P_{4\ell}(j_E)) =: -N_\ell$, where N_ℓ is divisible by ℓ or not a square modulo ℓ since $\ell \equiv 3 \bmod 4$. In particular, N_ℓ has a prime divisor p with $p = \ell$ or $\left(\frac{p}{\ell}\right) = -1$.

Now we want to construct and bound ℓ. We have to make sure that every prime p with bad reduction is a square modulo ℓ. Furthermore, we want ℓ to be congruent to 7 modulo 8 and last but not least we want ℓ to be at least as large as $\max(11, M, B_E)$. This must be a supersingular prime for E by Elkies [Elk87]. By adding more congruence conditions $\left(\frac{p'}{\ell}\right) = 1$ for finitely many primes p', we can rule out that ℓ is in a finite prescribed set. Since we want to exclude all number $p \leq n$, we add the condition $\left(\frac{p'_i}{\ell}\right) = 1$ for all $p'_i \leq n$.

With the Chinese Remainder Theorem we can put the equations

$$\left(\frac{p_i}{\ell}\right) = 1 \text{ for all primes } p_i \mid \mathrm{rad}(6N)$$
$$\left(\frac{p'_i}{\ell}\right) = 1 \text{ for all primes } p'_i \leq n$$
$$\text{and } \ell \equiv 7 \bmod 8$$

into one equation

$$\ell \equiv a \bmod q \tag{4.6}$$

for some a which is coprime to q with $24 \leq q \leq 24\mathrm{rad}(N)e^{\vartheta(n)} \leq 24Ne^{\vartheta(n)}$.

By Corollary 4.7 and with $24Ne^{\vartheta(n)} > 10^5$ (this is true since n and N are both at least 11) we know that there is a prime ℓ satisfying $\ell \equiv a \bmod q$ with

$$\ell \leq e^{\frac{1}{180}24Ne^{\vartheta(n)}} = e^{\frac{2}{15}Ne^{\vartheta(n)}}.$$

Together with Lemma 4.5 this gives us a supersingular prime p which is bounded from above by

$$p \leq e^{2\cdot 10^5\sqrt{\ell}(\log \ell)^2 h^*(j_E)}.$$

For better readability we take the logarithm

$$\begin{aligned}\log p &\leq 2 \cdot 10^5 \sqrt{\ell} (\log \ell)^2 h^*(j_E) \\ &\leq 2 \cdot 10^5 e^{\frac{1}{15} N e^{\vartheta(n)}} (\frac{2}{15} N e^{\vartheta(n)})^2 h^*(j_E) \\ &\leq 4 \cdot 10^3 e^{\frac{1}{15} N e^{\vartheta(n)}} (N e^{\vartheta(n)})^2 h^*(j_E),\end{aligned}$$

which is what we wanted to prove. □

If one does not attach importance to explicit constants, we can also use Linnik's Theorem with an explicit exponent as proved by Xylouris [Xyl11b] in Theorem 2.1. We get the following better bound.

Corollary 4.10
With the notation from the theorem there exists an effectively computable constant c such that

$$\log p \leq c q^{\frac{5}{2}} (\log q)^2 h^*(j_E).$$

Proof
We go back to the proof of the theorem before and replace the part where we use the explicit result on primes in arithmetic progressions by Xylouris' effective version of Linnik's Theorem (equation (4.6)). It gives us

$$\ell \leq c' q^5$$

with an effective constant c'. So we get

$$\begin{aligned}\log p &\leq 2.3 \cdot 10^{11} \sqrt{c' \cdot q^5} (\log(c' q^5))^2 h^*(j_E) \\ &\leq c q^{\frac{5}{2}} (\log q)^2 h^*(j_E).\end{aligned}$$

□

With a result of von Känel we can bound the height of the j-invariant by the conductor.

Theorem 4.11 ([vK14], equations 2.1 and 3.6 and [vM16], Proposition 6.8)
Let E be an elliptic curve over $\mathbb{Q}$ with j-invariant j_E and conductor N. Then we have

$$\begin{aligned}h(j_E) &\leq 12 h_F(E) + 6 \log \max(1, h_F(E)) + 75.84 \\ &\leq h(E) + 6 \log \max(1, h(E)) + 75.84\end{aligned}$$

where $h_F(E)$ is the stable Faltings height and $h(E)$ is the relative Faltings height of E and

$$h(F) \leq \frac{N}{12} \log N + \frac{N}{32} \log \log \log N + \frac{N}{18} + 2\pi + \frac{1}{2} \log \frac{163}{\pi}.$$

Corollary 4.12
Let E be an elliptic curve over $\mathbb{Q}$ with j-invariant j_E and conductor N. Then we have

$$h^*(j_E) \leq 10N \log N.$$

Proof
Since $h^*(j_E)$ differs from $h(j_E)$ only when $h(j_E) = 0$ and since $10N \log N$ is always greater than $\log 2$ (since $N \geq 2$) it is enough to show that $h(j_E) \leq 10N \log N$.

We want to simplify the bound from Theorem 4.11 and use the fact that the conductor N of an elliptic curve over $\mathbb{Q}$ is at least 11. We get

$$\begin{aligned} 12h_E &\leq N \log N + \frac{3N}{8} \log \log \log N + \frac{2N}{3} + 99.1 \\ &\leq N \log N + \frac{3N}{8} \log N + \frac{2N}{3} + 99.1 \\ &\leq N \log N + \frac{3}{8} N \log N + \frac{2}{3 \log 11} N \log N + \frac{99.1}{11 \log 11} N \log N \\ &\leq 5.42 N \log N \end{aligned}$$

and

$$\begin{aligned} 6 \log \max(1, h_E) &\leq 6 \log(\frac{6}{12} N \log N) \\ &\leq 6 \log(N^2) \\ &\leq \frac{6}{11} N \log(N^2) \\ &\leq \frac{12}{11} N \log N. \end{aligned}$$

Altogether we get

$$\begin{aligned} h(j_E) &\leq 12h_E + 6 \log \max(1, h_E) + 75.84 \\ &\leq 6N \log N + \frac{12}{11} N \log N + \frac{75.84}{11 \log 11} N \log N \\ &\leq 10N \log N. \end{aligned}$$

which is the desired bound. □

Now we can reformulate our result with dependence only on the conductor.

Theorem 4.13
Let E be an elliptic curve with conductor N. Let $M \in \mathbb{N}$ and $n = \max(M, 11(N \log N)^2)$. Then there exists a supersingular prime p of E such that $p \geq n$ and

$$\log p \leq 4 \cdot 10^4 e^{\frac{1}{15} N e^{\vartheta(n)}} (N e^{\vartheta(n)})^2 N \log N.$$

Proof
Let j_E be the j-invariant of E. First, we prove that $B_E \leq (6N \log N)^2$.

$$\begin{aligned} B_E &\leq \left(\frac{\log \max(|j_E|, 1)}{\pi} + 1 \right)^2 \\ &\leq \left(\frac{h^*(j_E)}{\pi} + 1 \right)^2 \\ &\leq \left(\frac{10N \log N}{\pi} + \frac{N \log N}{11 \log 11} \right)^2 \\ &\leq 11(N \log N)^2. \end{aligned}$$

With the bound for the height of the j-invariant from the above corollary we get the desired bound from Theorem 4.8. □

4.2 Handling the sum

4.2.1 Using a result of Mignotte

In this section we want to bound the sum in Proposition 3.13 from below. Our goal is to eventually show that this is negligible when compared to $\frac{\log p}{2p^8}$. This section does not involve elliptic curves, it deals only with algebraic numbers of small height. We start with the following lemma.

Lemma 4.14
Let $\beta \in \overline{\mathbb{Q}}^*$ of degree $d \geq 2$ and let $0 < \varepsilon \leq \frac{1}{2}$. Then

$$\frac{1}{[\mathbb{Q}(\beta) : \mathbb{Q}]} \sum_{\tau : \mathbb{Q}(\beta) \hookrightarrow \mathbb{C}} \log |\tau(\beta) - 1| \leq 2(\varepsilon |\log \varepsilon| + |\log(1-\varepsilon)|) + \frac{2}{\varepsilon d} \log d + (1 + \frac{1}{\varepsilon}) h(\beta),$$

where τ runs over all embeddings of $\mathbb{Q}(\beta)$ into $\mathbb{C}$.

Proof
Let $F(x) = a_d x^d + \cdots + a_0 = a_d \cdot (x - \beta_1) \cdot \cdots \cdot (x - \beta_d)$ be the unique integral polynomial of degree $d = [\mathbb{Q}(\beta) : \mathbb{Q}]$ that vanishes at β with $a_d \geq 1$ and $a_0, ..., a_d$ coprime. Since

$$0 \neq |F(1)| = |a_d| \cdot \prod_{i=1}^{d} |\beta_i - 1|$$

we get

$$\begin{aligned}\frac{1}{d}\log|F(1)| &= \frac{\log|a_d|}{d} + \frac{1}{d}\sum_{i=1}^{d}\log|\beta_i - 1| \\ &\geq \frac{1}{d}\sum_{i=1}^{d}\log|\beta_i - 1| \\ &= \frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]}\sum_{\tau:\mathbb{Q}(\beta)\hookrightarrow\mathbb{C}}\log|\tau(\beta)-1|. \end{aligned} \tag{4.7}$$

So it is enough to bound $|F(1)|$ in order to prove the Lemma.

For any polynomial $G = g_n x^n + \cdots + g_0 \in \mathbb{Z}[x]$ we define its height as $H(G) := \max_i |g_i|$. Furthermore, let $G_k := \frac{1}{k!}\frac{d^k G}{dx^k} = \sum_{i=k}^{n}\binom{i}{k} g_i x^{i-k} \in \mathbb{Z}[x]$ and $D \geq d$. We will fix D later in terms of ε and d. By Mignotte's Theorem B in [Mig89] we can find a polynomial $A(x) = \sum_{i=0}^{D-d} a_i x^i \in \mathbb{Z}[x] \setminus \{0\}$ of degree at most $D-d$ such that

$$H(A \cdot F) \leq ((D+1)^{\frac{d}{2}} H(\beta)^{Dd})^{\frac{1}{D+1-d}}. \tag{4.8}$$

Let $k \in \mathbb{N}_0$ be the multiplicity of the zero at 1 of A. Since the degree of A is at most $D-d$ we have $k \leq D-d$. Then $A_{k-i}(1) = 0$ for all positive $i \leq k$ and $A_k(1) \neq 0$. As $A_k(1) \in \mathbb{Z}$ we find $|A_k(1)| \geq 1$ and thus by the Leibniz formula we get

$$\begin{aligned}|F(1)| &\leq |A_k(1)||F(1)| \\ &= |(A \cdot F)_k(1)| \\ &\leq (D-k+1)H((A \cdot F)_k) \\ &\leq (D-k+1)\binom{D}{k}H(A \cdot F). \end{aligned} \tag{4.9}$$

By putting inequalities (4.7), (4.8) and (4.9) together we get

$$\begin{aligned}\frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]}\sum_{\tau:\mathbb{Q}(\beta)\hookrightarrow\mathbb{C}}\log|\tau(\beta)-1| &\leq \frac{1}{d}\log|F(1)| \\ &\leq \frac{1}{d}\log\left((D-k+1)\binom{D}{k}H(A\cdot F)\right) \\ &\leq \frac{1}{d}\log\left((D-k+1)\binom{D}{k}((D+1)^{\frac{d}{2}}H(\beta)^{Dd})^{\frac{1}{D+1-d}}\right) \\ &\leq \frac{1}{d}\log\left(\binom{D}{k}(D+1)^{\frac{d}{2(D+1-d)}+1}H(\beta)^{\frac{Dd}{D+1-d}}\right).\end{aligned}$$

The right hand side equals

$$\frac{1}{d}\log\binom{D}{k} + \left(\frac{1}{2(D+1-d)} + \frac{1}{d}\right)\log(D+1) + \frac{D}{D+1-d}h(\beta).$$

Note that $\varepsilon d \leq \varepsilon[(1+\varepsilon)d]$ and so with $D := [(1+\varepsilon)d]$ we have

$$k \leq D - d \leq \varepsilon d \leq \varepsilon[(1+\varepsilon)d].$$

So we can apply Lemma 16.19 of [FG06] with $q = \varepsilon > 0$ and $n = D$. We get $\binom{[(1+\varepsilon)d]}{k} \leq 2^{-(1+\varepsilon)d(\varepsilon\log\varepsilon+(1-\varepsilon)\log(1-\varepsilon))}$. Since $\varepsilon < 1$ we can write $|\log\varepsilon|$ instead of $-\log\varepsilon$ and $|\log(1-\varepsilon)|$ instead of $-\log(1-\varepsilon)$. So we can bound the above expression by

$$((1+\varepsilon)\varepsilon|\log\varepsilon| + (1-\varepsilon^2)|\log(1-\varepsilon)|)\log 2 + \frac{1+2\varepsilon}{2\varepsilon d}\log((1+\varepsilon)d+1) + (1+\frac{1}{\varepsilon})h(\beta).$$

We start by bounding the first summand:

$$\begin{aligned}((1+\varepsilon)\varepsilon|\log\varepsilon| + (1-\varepsilon^2)|\log(1-\varepsilon)|)\log 2 &\leq (\frac{3}{2}\varepsilon|\log\varepsilon| + |\log(1-\varepsilon)|)\log 2\\ &\leq 2(\varepsilon|\log\varepsilon| + |\log(1-\varepsilon)|).\end{aligned}$$

The second summand can also be bounded further:

$$\begin{aligned}\frac{1+2\varepsilon}{2\varepsilon d}\log((1+\varepsilon)d+1) &\leq \frac{2}{2\varepsilon d}\log(d^2)\\ &= \frac{2}{\varepsilon d}\log d.\end{aligned}$$

We put both bounds together and get

$$2(\varepsilon|\log\varepsilon| + |\log(1-\varepsilon)|) + \frac{2}{\varepsilon d}\log d + (1+\frac{1}{\varepsilon})h(\beta) \tag{4.10}$$

as an upper bound for $\frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]}\sum_{\tau:\mathbb{Q}(\beta)\hookrightarrow\mathbb{C}}\log|\tau(\beta)-1|$.

□

Later, we will fix an ε and then get an explicit bound. But first, we want to look at the terms separately.

Lemma 4.15
Let $0 < x \leq \frac{1}{2}$. Then

$$-2(x\log x + \log(1-x)) \leq -(2+\frac{4}{\log 2})x\log x.$$

Proof
We have $\log(1+t) \leq t$ for all $t \geq 0$ and

$$-\log(1-x) = \log\frac{1}{1-x} = \log(1+\frac{x}{1-x}).$$

So

$$-\log(1-x) \leq \frac{x}{1-x} \leq 2x$$

since $x \leq \frac{1}{2}$. The bound then follows from $2x \leq -2\frac{x\log x}{\log 2}$ as $-\frac{\log x}{\log 2} \geq 1$.

□

For our purpose the following corollary is sufficient.

Corollary 4.16
Let $0 < x \leq \frac{1}{2}$ *and* $0 < \gamma < 1$. *We have*

$$-2(x \log x + \log(1-x)) \leq 8\frac{1}{\gamma e} x^{1-\gamma}.$$

Proof
We use the lemma from above and want to show that $-x \log x \leq \frac{1}{\gamma e} x^{1-\gamma}$. We use basic calculus to get the maximum value. We compute the derivative with respect to x as

$$(-x^{\gamma} \log x)' = -x^{\gamma-1}(\gamma \log x + 1).$$

In our interval, this is zero if and only if

$$x = e^{-\frac{1}{\gamma}}.$$

Since we have $-(\frac{1}{2})^{\gamma-1}(\gamma \log \frac{1}{2} + 1) < 0$ for all $0 < \gamma < 1$, the slope of $-x^{\gamma} \log x$ changes its sign at $x = e^{-\frac{1}{\gamma}}$ from positive to negative and so we have a maximum. Finally, we have

$$-x^{\gamma} \log x \leq -e^{-\frac{1}{\gamma}\gamma} \log(e^{-\frac{1}{\gamma}}) = \frac{1}{\gamma e}$$

which after multiplying by the positive value $x^{1-\gamma}$ gives the desired result.

□

We need a similar result for the second summand.

Lemma 4.17
Let $0 < \eta < 1$ *and* $d \geq 16$. *Then for every* $x > \frac{1}{4d}\left(\frac{\log\log d}{\log d}\right)^3$ *we have*

$$\frac{\log d}{d} \leq \frac{19}{\eta^4} x^{1-\eta}.$$

Remark 4.18
The constraint $d \geq 16$ guarantees that $\frac{\log\log d}{\log d}$ is a decreasing function.

Proof
Let us look at the function $4\frac{(\log d)^4}{d^{\eta}}$. To see that it is bounded from above we compute the derivative with respect to d:

$$\left(4\frac{(\log d)^4}{d^{\eta}}\right)' = \frac{4}{d^{1+\eta}}(\log d)^3(4 - \eta \log d).$$

This is zero if and only if $d = e^{\frac{4}{\eta}}$. Since the derivative changes sign at $e^{\frac{4}{\eta}}$, our extremum is a maximum. So $4\frac{(\log e^{\frac{4}{\eta}})^4}{(e^{\frac{4}{\eta}})^\eta} = \frac{4^5}{e^4\eta^4}$ is an upper bound for $4\frac{(\log d)^4}{d^\eta}$ and we get

$$\begin{aligned}
\frac{19}{\eta^4} &\geq \frac{4^5}{e^4\eta^4} \\
&\geq 4\frac{(\log d)^4}{d^\eta} \\
&\geq 4^{1-\eta}\frac{(\log d)^{4-3\eta}}{d^\eta(\log\log d)^{3-3\eta}} \\
&= \frac{\log d}{d}\left(4d\left(\frac{\log d}{\log\log d}\right)^3\right)^{1-\eta} \\
&\geq \frac{\log d}{d}\left(\frac{1}{x}\right)^{1-\eta}
\end{aligned}$$

which gives the desired inequality.

□

In the next lemma we combine all of the previous results of this section.

Lemma 4.19
Let $\delta < \frac{1}{2}$ and let $\beta \in \overline{\mathbb{Q}^*} \setminus \mu_\infty$ be such that $[\mathbb{Q}(\beta) : \mathbb{Q}] \geq 16$ and $h(\beta)^{\frac{1}{2}} \leq \frac{1}{2}$. Then we have

$$\frac{1}{[\mathbb{Q}(\beta) : \mathbb{Q}]} \sum_{\tau : \mathbb{Q}(\beta) \hookrightarrow \mathbb{C}} \log|\tau(\beta) - 1| \leq \frac{40}{\delta^4} h(\beta)^{\frac{1}{2}-\delta}. \tag{4.11}$$

Proof
Set $\varepsilon = h(\beta)^{\frac{1}{2}}$. Then Lemma 4.14 gives

$$\begin{aligned}
&\frac{1}{[\mathbb{Q}(\beta) : \mathbb{Q}]} \sum_{\tau : \mathbb{Q}(\beta) \hookrightarrow \mathbb{C}} \log|\tau(\beta) - 1| \\
&\leq -2(\varepsilon\log\varepsilon + \log(1-\varepsilon)) + \frac{2}{\varepsilon d}\log d + (1 + \frac{1}{\varepsilon})h(\beta) \\
&\leq -2(h(\beta)^{\frac{1}{2}}\log h(\beta)^{\frac{1}{2}} + \log(1 - h(\beta)^{\frac{1}{2}})) + \frac{2\log d}{h(\beta)^{\frac{1}{2}} d} + h(\beta)^{\frac{1}{2}} + h(\beta)^{\frac{1}{2}}.
\end{aligned}$$

Now since $h(\beta)^{\frac{1}{2}} \leq \frac{1}{2}$, we can apply Corollary 4.16 to the first term. By the main theorem of [Vou96] we also have $h(\beta) > \frac{1}{4d}\left(\frac{\log\log d}{\log d}\right)^3$ and so we can apply Lemma 4.17 to the second term and for any $0 < \gamma, \eta < 1$ we get:

$$\frac{1}{[\mathbb{Q}(\beta) : \mathbb{Q}]} \sum_{\tau : \mathbb{Q}(\beta) \hookrightarrow \mathbb{C}} \log|\tau(\beta) - 1| \leq \frac{8}{\gamma e} h(\beta)^{\frac{1}{2}(1-\gamma)} + \frac{38}{\eta^4} h(\beta)^{\frac{1}{2}-\eta} + 2h(\beta)^{\frac{1}{2}}.$$

Now we set $\gamma := 2\delta$ and $\eta := \delta$ and get

$$\begin{aligned}\frac{8}{\gamma e}h(\beta)^{\frac{1}{2}(1-\gamma)} + \frac{38}{\eta^4}h(\beta)^{\frac{1}{2}-\eta} + 2h(\beta)^{\frac{1}{2}} &\leq \frac{1}{\delta^4}h(\beta)^{\frac{1}{2}-\delta}(\frac{8}{2e}\delta^3 + 38 + 2\delta^4) \\ &\leq \frac{40}{\delta^4}h(\beta)^{\frac{1}{2}-\delta},\end{aligned}$$

which is what we wanted to show. □

4.2.2 An alternative approach to handle the sum

As the title of this section already reveals, we want to give an alternative approach to handle the sum in Proposition 3.13. This approach was communicated by Amoroso and appears in [ADZ14]. We will not bound the sum directly but we will try to get rid of the sum before it even occurs. For this we will quote and try to improve a result of Habegger. Recall the notations and conventions of Chapter 3: We have an ellipticv curve E without complex multiplication, p a prime satisfying 5.1 and 5.2.

The following Lemma is the result we want to improve.

Lemma 4.20 ([Hab13], Lemma 4.2)
Under the assumptions from above, let $N \in \mathbb{N}$ and suppose $p|N$ and $\alpha \in \mathbb{Q}_q(N)^*$. Then for all $\psi \in \mathrm{Gal}(\mathbb{Q}_q(N)/\mathbb{Q}_q(N/p))$

$$|\psi(\alpha)^q - \alpha^q|_p \leq p^{-1}\max(1, |\psi(\alpha)|_p)^q \max(1, |\alpha|_p)^q.$$

We want to replace the p^{-1} in the lemma by something smaller.

Lemma 4.21
Let $p|N$ and $\alpha \in \mathbb{Q}_q(N)^*$. Then for all $\psi \in \mathrm{Gal}(\mathbb{Q}_q(N)/\mathbb{Q}_q(N/p))$ and $\lambda \in \mathbb{N} \setminus \{0\}$ we have

$$|(\psi(\alpha)^q)^{p^\lambda} - (\alpha^q)^{p^\lambda}|_p \leq p^{-s}\max(1, |\psi(\alpha)|_p)^{qt} \max(1, |\alpha|_p)^{qt}$$

with $s = 1 + \lambda$ and $t = p^\lambda$.

The proof is essentially the same as in [ADZ14], Lemma 2.1.

Proof
Consider

$$|(\psi(\alpha)^q)^{p^\lambda} - (\alpha^q)^{p^\lambda}|_p = |\psi(\alpha)^q - \alpha^q|_p \prod_{j=1}^{\lambda} \prod_{\substack{\zeta \in \overline{\mathbb{Q}}_p \\ \mathrm{ord}\,(\zeta) = p^j}} |\psi(\alpha)^q - \zeta\alpha^q|_p.$$

By [Neu99], Proposition 7.13 (i) (p. 159) and Theorem 4.8 (p. 131), we have $|1-\zeta|_p = p^{-\frac{1}{p^{j-1}(p-1)}}$ if ord $\zeta = p^j$ and $j \geq 1$, so we get:

$$\begin{aligned}
|\psi(\alpha)^q - \zeta\alpha^q|_p &= |\psi(\alpha)^q - \alpha^q + \alpha^q - \zeta\alpha^q|_p \\
&\leq \max(|\psi(\alpha)^q - \alpha^q|_p, |1-\zeta|_p|\alpha^q|_p) \\
&\overset{\text{Lemma 4.20}}{\leq} \max(p^{-1}\max(1,|\psi(\alpha)|_p)^q \max(1,|\alpha|_p)^q, |1-\zeta|_p|\alpha^q|_p) \\
&= \max(p^{-1}\max(1,|\psi(\alpha)|_p)^q \max(1,|\alpha|_p)^q, p^{-\frac{1}{p^{j-1}(p-1)}}|\alpha^q|_p) \\
&\leq p^{-\frac{1}{p^{j-1}(p-1)}} \max(1,|\psi(\alpha)|_p)^q \max(1,|\alpha|_p)^q
\end{aligned}$$

So we get

$$|(\psi(\alpha)^q)^{p^\lambda} - (\alpha^q)^{p^\lambda}|_p \leq p^{-s}(\max(1,|\psi(\alpha)|_p)^q \max(1,|\alpha|_p)^q)^t,$$

where

$$\begin{aligned}
s &= 1 + \sum_{j=1}^{\lambda} \sum_{\substack{\zeta \in \overline{\mathbb{Q}}_p \\ \text{ord }(\zeta)=p^j}} \frac{1}{p^{j-1}(p-1)} \\
&= 1 + \sum_{j=1}^{\lambda} p^{j-1}(p-1)\frac{1}{p^{j-1}(p-1)} \\
&= 1 + \lambda
\end{aligned}$$

and

$$\begin{aligned}
t &= 1 + \sum_{j=1}^{\lambda} \sum_{\substack{\zeta \in \overline{\mathbb{Q}}_p \\ \text{ord }(\zeta)=p^j}} 1 \\
&= 1 + \sum_{j=1}^{\lambda} p^{j-1}(p-1) \\
&= 1 + (p-1)\frac{p^\lambda - 1}{p-1} \\
&= p^\lambda.
\end{aligned}$$

□

The next step is to reformulate Lemma 5.3 of [Hab13]. We try to get a similar result by using the above Lemmas.

Lemma 4.22
Let $\lambda \in \mathbb{N}$. We assume $p|N$ and let $n \geq 1$ be the greatest integer such that p^n divides N. Let $Q(n) = \begin{cases} q & \text{if } n \geq 2, \\ (q-1)q & \text{if } n = 1 \end{cases}$. If $\alpha \in \mathbb{Q}(N)$ satisfies $\alpha^{Q(n)p^\lambda} \notin \mathbb{Q}_q(N/p)$,

then

$$h(\alpha) \geq \frac{1}{2p^{\lambda}p^2}\left(\frac{(1+\lambda)\log p}{p^6} - \log 2\right). \tag{4.12}$$

We follow the proof of Lemma 5.3 of [Hab13] very closely and use our Lemma 4.21 instead of Lemma 4.2 in [Hab13].

Proof
For brevity, we set $Q = Q(n)$. By hypothesis we may choose $\psi \in \mathrm{Gal}(\mathbb{Q}_q(N)/\mathbb{Q}_q(N/p))$ with $\psi(\alpha^{Qp^{\lambda}}) \neq \alpha^{Qp^{\lambda}}$. We note that $\alpha \neq 0$. We define

$$x = \psi(\alpha^{Qp^{\lambda}}) - \alpha^{Qp^{\lambda}} \in \mathbb{Q}(N)$$

and observe $x \neq 0$ by our choice of ψ. So

$$\sum_w d_w \log |x|_w = 0 \tag{4.13}$$

by the product formula. Say $G = \{\sigma \in \mathrm{Gal}(\mathbb{Q}(N)/\mathbb{Q}) | \sigma\psi\sigma^{-1} = \psi\}$ and v is the place of $\mathbb{Q}(N)$ induced by $|\cdot|_p$. Let $\sigma \in G$. The place σv of $\mathbb{Q}(N)$ is defined by $|\sigma(y)|_{\sigma v} = |y|_v$ for all $y \in \mathbb{Q}(N)$. So $|(\sigma\psi\sigma^{-1})(\alpha^Q)^{p^{\lambda}} - (\alpha^Q)^{p^{\lambda}}|_{\sigma v} = |\psi(\sigma^{-1}(\alpha^Q)^{p^{\lambda}}) - \sigma^{-1}(\alpha^Q)^{p^{\lambda}}|_v$. By definition we have $q|Q$, so we may apply Lemma 4.21 to $\sigma^{-1}(\alpha)^{\frac{Q}{q}}$. This implies

$$\begin{aligned}
|(\sigma\psi\sigma^{-1})(\alpha^{Qp^{\lambda}}) - \alpha^{Qp^{\lambda}}|_{\sigma v} &= |\psi(\sigma^{-1}(\alpha^Q))^{p^{\lambda}} - \sigma^{-1}(\alpha^Q)^{p^{\lambda}}|_v \\
&\leq p^{-(\lambda+1)} \max(1, |\psi(\sigma^{-1}(\alpha)^{\frac{Q}{q}})|_v)^{qp^{\lambda}} \max(1, |\sigma^{-1}(\alpha)^{\frac{Q}{q}}|_v)^{qp^{\lambda}} \\
&\leq p^{-(\lambda+1)} \max(1, |(\sigma\psi\sigma^{-1})(\alpha)|_{\sigma v})^{Qp^{\lambda}} \max(1, |\alpha|_{\sigma v})^{Qp^{\lambda}}.
\end{aligned}$$

Now $\sigma\psi\sigma^{-1} = \psi$ since $\sigma \in G$. Therefore,

$$|x|_w \leq p^{-(\lambda+1)} \max(1, |\psi(\alpha)|_w)^{Qp^{\lambda}} \max(1, |\alpha|_w)^{Qp^{\lambda}} \text{ for all } w \in Gv. \tag{4.14}$$

If w is an arbitrary finite place of $\mathbb{Q}(N)$, the ultrametric triangle inequality implies

$$|x|_w \leq \max(1, |\psi(\alpha)|_w)^{Qp^{\lambda}} \max(1, |\alpha|_w)^{Qp^{\lambda}}. \tag{4.15}$$

Say w is an infinite place. Then the triangle inequality gives

$$\begin{aligned}
|x|_w &\leq |\psi(\alpha)|_w^{Qp^{\lambda}} + |\alpha|_w^{Qp^{\lambda}} \\
&\leq 2\max(1, |\psi(\alpha)|_w)^{Qp^{\lambda}} \max(1, |\alpha|_w)^{Qp^{\lambda}}.
\end{aligned} \tag{4.16}$$

We split the sum (4.13) up into the finite places in Gv, the remaining finite places and the infinite places. The estimates (4.14), (4.15) and (4.16) together with the

product formula (4.13) imply

$$\begin{aligned}
0 \leq & \sum_{w \in Gv} d_w \log(p^{-(\lambda+1)} \\
& + \sum_{w \nmid \infty} d_w \log(\max(1, |\psi(\alpha)|_w)^{Qp^\lambda} \max(1, |\alpha|_w)^{Qp^\lambda}) \\
& + \sum_{w | \infty} d_w \log(2 \max(1, |\psi(\alpha)|_w)^{Qp^\lambda} \max(1, |\alpha|_w)^{Qp^\lambda}) \\
\leq & \sum_{w \in Gv} d_w \log p^{-(\lambda+1)} \\
& + \sum_{w} d_w \log(\max(1, |\psi(\alpha)|_w)^{Qp^\lambda} \max(1, |\alpha|_w)^{Qp^\lambda}) + \sum_{w | \infty} d_w \log 2 \\
\leq & -(\lambda+1)|Gv| d_v \log p + \sum_{w} d_w \log(\max(1, |\psi(\alpha)|_w)^{Qp^\lambda} \max(1, |\alpha|_w)^{Qp^\lambda}) + \sum_{w | \infty} d_w \log 2.
\end{aligned}$$

Notice that all local degrees d_w equal d_v whenever $w \in Gv$. By Lemma 5.2 of [Hab13], we have $|Gv| \geq \frac{[\mathbb{Q}(N):\mathbb{Q}]}{d_v p^4}$ hence we can divide the whole expression by $[\mathbb{Q}(N) : \mathbb{Q}]$ and get

$$\begin{aligned}
\frac{(\lambda+1)\log p}{p^4} &\leq Qp^\lambda (h(\psi(\alpha)) + h(\alpha)) + \log 2 \\
&= 2Qp^\lambda h(\alpha) + \log 2.
\end{aligned}$$

With $p^2 \leq Q \leq p^4$ and we get

$$\begin{aligned}
h(\alpha) &\geq \frac{(\lambda+1)\log p}{2p^\lambda p^8} - \frac{\log 2}{2p^\lambda p^2} \\
&= \frac{1}{2p^\lambda p^2} \left(\frac{(\lambda+1)\log p}{p^6} - \log 2 \right) \\
&= \frac{1}{2p^\lambda p^2} \left(\frac{(1+\lambda)\log p}{p^6} - \log 2 \right).
\end{aligned}$$

□

Corollary 4.23
In the same setting as in the above lemma, but with $\lambda = p^6$ we have

$$h(\alpha) \geq \frac{\log \frac{p}{2}}{2p^{p^6+2}}$$

Proof
We just continue where the above proof ended and set $\lambda = p^6$.

$$h(\alpha) \geq \frac{1}{2p^{p^6}p^2}\left(\frac{(1+p^6)\log p}{p^6} - \log 2\right) \tag{4.17}$$

$$\geq \frac{1}{2p^{p^6+2}}(\log p - \log 2) \tag{4.18}$$

$$\geq \frac{\log \frac{p}{2}}{2p^{p^6+2}}. \tag{4.19}$$

□

This approach using p-adic amplification leads to worse dependency on p when compared to the equidistribution approach in Section 4.2.1. So we stop here.

4.3 Putting everything together to get an explicit lower bound

We gathered all the results we need and are now able to prove the main theorems.

Theorem 4.24
Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication and let $p \geq 5$ be a supersingular prime of E such that the Galois representation $Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to Aut\, E[p]$ is surjective. Then for $\alpha \in \mathbb{Q}(E_{tor})^* \setminus \mu_\infty$ we have

$$h(\alpha) \geq \frac{(\log p)^5}{10^{21} p^{44}}.$$

Proof
Without loss of generality, assume that $h(\alpha) \leq \frac{1}{40p^4}$.

Proposition 3.13 gives us $\beta \in \overline{\mathbb{Q}}^* \setminus \mu_\infty$ with $h(\beta) \leq 10p^4 h(\alpha)$ and

$$h(\alpha) \geq \frac{1}{5}\left(\frac{\log p}{2p^8} - \max\Big\{0, \frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]} \sum_{\tau:\mathbb{Q}(\beta)\hookrightarrow\mathbb{C}} \log|\tau(\beta)-1|\Big\}\right).$$

We want to distinguish two cases:

Case 1: $\deg \beta \geq 16$.

Here we can use Lemma 4.19 with $\delta = \frac{3}{10}$ and together with $h(\beta) \leq 10p^4 h(\alpha) \leq \frac{1}{4}$ we get

$$\begin{aligned} h(\alpha) &\geq \frac{1}{5}\left(\frac{\log p}{2p^8} - \frac{40}{(\frac{3}{10})^4}(10p^4 h(\alpha))^{\frac{1}{5}}\right) \\ &\geq \frac{1}{5}\left(\frac{\log p}{2p^8} - 4.94 \cdot 10^3 (10p^4 h(\alpha))^{\frac{1}{5}}\right). \end{aligned}$$

Since $h(\alpha) \leq 1$ we can make use of the fact that $h(\alpha)^{\frac{1}{5}} \geq h(\alpha)$. Then we find that

$$h(\alpha)^{\frac{1}{5}} + \frac{4.94}{5} 10^3 (10p^4 h(\alpha))^{\frac{1}{5}} \geq \frac{\log p}{10p^8},$$

which gives us

$$h(\alpha) \geq \left(\frac{1}{1 + \frac{4.94}{5} 10^3 (10p^4)^{\frac{1}{5}}} \frac{\log p}{10p^8}\right)^5.$$

We can simplify this and get

$$\begin{aligned} h(\alpha) &\geq \left(\frac{1}{1 + \frac{4.94}{5} 10^3 (10p^4)^{\frac{1}{5}}} \frac{\log p}{10p^8} \right)^5 \\ &\geq \left(\frac{1}{10^3 (10p^4)^{\frac{1}{5}}} \frac{\log p}{10p^8} \right)^5 \\ &\geq \frac{(\log p)^5}{10^{21} p^{44}}. \end{aligned}$$

Case 2: $d \leq 15$.

In this case we easily get an estimate with Corollary 2 of [Vou96]:

$$\begin{aligned} h(\beta) &> \frac{2d}{(\log(3d))^3} \\ &\geq \frac{1}{(\log(45))^3} \\ &\geq 0.02. \end{aligned}$$

This is always bigger than our bound from above so we proved the theorem.

□

The case of complex multiplication is even easier:

Theorem 4.25
Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication. Then for $\alpha \in \mathbb{Q}(E_{tor})^* \setminus \mu_\infty$ we have

$$h(\alpha) \geq 3^{-14}.$$

Proof
If E has complex multiplication, then there exists a quadratic number field K such that $K(E_{\text{tor}})/K$ is abelian. Theorem 1.2 of [AZ10] tells us that the height of $\alpha \in K(E_{\text{tor}})^* \setminus \mu_\infty$ is bounded from below by 3^{-14} which is always bigger than the bound in the theorem. □

Since for a semistable elliptic curve the Galois representation is surjective for all $p \geq 11$ (Theorem 4 of [Maz78]) we have the following corollary.

Corollary 4.26
Let E be a semistable elliptic curve defined over $\mathbb{Q}$ without complex multiplication and let $p \geq 11$ be a supersingular prime of E. Then for $\alpha \in \mathbb{Q}(E_{tor})^* \setminus \mu_\infty$ we have

$$h(\alpha) \geq \frac{(\log p)^5}{10^{21} p^{44}}.$$

Furthermore, we also have a bound for the smallest supersingular prime of E. Recall the definition of B_E in Lemma 4.3. With $M = 11$, Theorem 4.13 gives us the next corollary. We will use the expression exp for the exponential function since it improves readibility.

Corollary 4.27

Let E be a semistable elliptic curve defined over $\mathbb{Q}$ of conductor N. Let $\alpha \in \mathbb{Q}(E_{tor})^* \setminus \mu_\infty$. Then with and $n = \max(11, B_E)$ we have

$$h(\alpha) \geq \exp(-2 \cdot 10^7 \exp(\frac{1}{15} N \exp(\vartheta(n)))(N \exp(\vartheta(n)))^2 N \log N)$$

Proof

For elliptic curves with complex multiplication, we have $h(\alpha)$ $geq 3^{-14}$ which is always greater than the above bound, so assume E does not have complex multiplication.

With $p \geq 11$, Theorem 4.24 and Theorem 4.13 we get

$$\begin{aligned}
h(\alpha) &\geq \frac{(\log p)^5}{10^{21} p^{44}} \\
&\geq \frac{(\log 11)^5}{10^{21}} \exp(-4 \cdot 10^5 \exp(\frac{1}{15} N \exp(\vartheta(n)))(N \exp(\vartheta(n)))^2 N \log N))^{44} \\
&\geq \frac{(\log 11)^5}{10^{21}} \exp(-1.9 \cdot 10^7 \exp(\frac{1}{15} N \exp(\vartheta(n)))(N \exp(\vartheta(n)))^2 N \log N) \\
&\geq \exp(-1.9 \cdot 10^7 \exp(\frac{1}{15} N \exp(\vartheta(n)))(N \exp(\vartheta(n)))^2 N \log N - 44) \\
&\geq \exp(-2 \cdot 10^7 \exp(\frac{1}{15} N \exp(\vartheta(n)))(N \exp(\vartheta(n)))^2 N \log N)
\end{aligned}$$

□

Theorem 4.2 of [LF16] gives us a bound for surjective primes: A prime $p \geq 10^7 \max\{985, \frac{1}{12} h(j_E) + 3\}^2$ will always be surjective.

Remark 4.28

In the next versions we do not have to care about the B_E since $n = 10^7 \max\{985, \frac{1}{12} h(j_E) + 3\}^2$ is always bigger than B_E: For $j_E = 0$ we have $B_E = 0$ which is always smaller than n. For $j_E \neq 0$ we have

$$\begin{aligned}
B_E &\leq \left(\frac{\log |j_E|}{2\pi}\right)^2 \\
&\leq \frac{h(j_E)^2}{40} \\
&\leq 10^7 \left(\frac{h(j_E)}{12}\right)^2 \\
&\leq 10^7 \left(\frac{h(j_E)}{12} + 3\right)^2 \\
&\leq n.
\end{aligned}$$

Here, we can get rid of the height of the j-invariant by bounding it via Theorem 4.11: $10^7 \max\{985, \frac{1}{12}h^*(j_E)+3\}^2 \leq 10^7 \max\{985, \frac{1}{12}(18N\log N)+3\}^2$.

Theorem 4.29
Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. Let $\alpha \in \mathbb{Q}(E_{tor})^* \setminus \mu_\infty$. Then with $n = 10^7 \max\{985, \frac{1}{12}(10N\log N)+3\}^2$ we have

$$h(\alpha) \geq \exp(-7.3 \cdot 10^7 \exp(\frac{1}{15}N\exp(\vartheta(n)))(N\exp\vartheta(n)))^2 N\log N).$$

Proof
For an elliptic curve without complex multiplication we have $h(\alpha) \geq 3^{-14}$ which is always larger than the above bound, so assume that E does not have complex multiplication.

By Theorem 4.13 with $M = n$ we find a supersingular prime $p \geq \max(n, 11(N\log N)^2) \geq 7 \cdot 10^3 \geq e^8$ for E such that

$$\log p \leq 4 \cdot 10^4 e^{\frac{1}{15}Ne^{\vartheta(n)}}(Ne^{\vartheta(n)})^2 N\log N.$$

Since $p \geq n$ we know by Theorem 3.16 that also the Galois representation is surjective. Hence we can use Theorem 4.24 and get

$$\begin{aligned}
h(\alpha) &\geq \frac{(\log p)^5}{10^{21}p^{44}} \\
&\geq 5 \cdot 10^{17} \exp(-44 \cdot 4 \cdot 10^4 \exp(\frac{1}{15}N\exp(\vartheta(n)))(N\exp\vartheta(n))^2 N\log N) \\
&\geq \exp(-41 \cdot 44 \cdot 4 \cdot 10^4 \exp(\frac{1}{15}N\exp(\vartheta(n)))(N\exp\vartheta(n))^2 N\log N) \\
&\geq \exp(-7.3 \cdot 10^7 \exp(\frac{1}{15}N\exp(\vartheta(n)))(N\exp\vartheta(n))^2 N\log N),
\end{aligned}$$

which proves the statement. □

If we are only interested in effective results, we can use Corollary 4.10 and get the following effective, non-explicit result.

Theorem 4.30
Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and j-invariant j_E. Let $\alpha \in \mathbb{Q}(E_{tor})^* \setminus \mu_\infty$. Then with $q = 4rad(6N)$ there is an effectively computable constant $c > 0$ such that

$$h(\alpha) \geq c\frac{(q^{\frac{5}{2}}(\log q)^2 h^*(j_E)))^5}{\left(e^{q^{\frac{5}{2}}(\log q)^2 h^*(j_E)}\right)^{44}}.$$

Proof
As usual, in the case of complex multiplication, we have $h(\alpha) \geq 3^{-14}$ which is a better bound than the above one, so we may assume that E does not have complex multiplication.

We use Theorem 4.24 together with Corollary 4.10 to get an effectively computable constant $c' > 0$ such that

$$\begin{aligned} h(\alpha) &\geq \frac{(q^{\frac{5}{2}}(\log q)^2 h^*(j_E)))^5}{\left(e^{cq^{\frac{5}{2}}(\log q)^2 h^*(j_E)}\right)^{44}} \\ &\geq \frac{(c'q^{\frac{5}{2}}(\log q)^2 h^*(j_E)))^5}{e^{(44c'q^{\frac{5}{2}}(\log q)^2 h^*(j_E))}} \\ &\geq c\frac{(q^{\frac{5}{2}}(\log q)^2 h^*(j_E)))^5}{e^{(q^{\frac{5}{2}}(\log q)^2 h^*(j_E))}}, \end{aligned}$$

which is what we wanted to show. □

4.4 Examples

In this section we want to give some examples of the height bound.

Example
Let $E : y^2 = x^3 + x$. Since E has complex multiplication, we can refer to the proof of Theorem 4.24. Then for all $\alpha \in \mathbb{Q}(E_{\text{tor}})^* \setminus \mu_\infty$ we have

$$h(\alpha) \geq 3^{-14}.$$

For the next example we cite a result of Rosser and Schönfeld.

Theorem 4.31 ([RS62])
For $x > 0$ we have $\vartheta(x) < 1.01624x$.

Example
Let $E : y^2 + y = x^3 - x^2 - 10x - 20$. By, the LMFDB [LMF13, Elliptic Curve 11.a2], this curve has the smallest possible conductor 11. With $n = 10^7 \max\{985, \frac{1}{12}(10N \log N) + 3\}^2 = 10^7 \cdot 985^2$ we can use Theorem 4.29. Then for all $\alpha \in \mathbb{Q}(E_{\text{tor}})^* \setminus \mu_\infty$

$$\begin{aligned} h(\alpha) &\geq \exp(-7.3 \cdot 10^7 \exp(\frac{1}{15} N \exp(\vartheta(n)))(N \exp(\vartheta(n)))^2 N \log N) \\ &\geq \exp(-7.3 \cdot 10^7 \exp(\frac{1}{15} 11 \exp(1.01624n))(11 \exp(1.01624n))^2 11 \log 11). \end{aligned}$$

Example
Let $E : y^2 + y = x^3 - x^2$. Then by [Elk87] the prime 19 is supersingular for E and by [LMF13, Elliptic Curve 11.a3], all primes but 5 are surjective. So for all $\alpha \in \mathbb{Q}(E_{\text{tor}})^* \setminus \mu_\infty$ we have

$$\begin{aligned} h(\alpha) &\geq \frac{(\log 19)^5}{10^{21} 19^{44}} \\ &\geq 10^{-66}. \end{aligned}$$

Example
Let $E : y^2 + xy + y = x^3 - x^2$. Then [LMF13, Elliptic Curve 53.a1], the prime 5 is supersingular and surjective. So for all $\alpha \in \mathbb{Q}(E_{\text{tor}})^* \setminus \mu_\infty$ we have

$$\begin{aligned} h(\alpha) &\geq \frac{(\log 5)^5}{10^{21} 5^{44}} \\ &\geq 10^{-51}. \end{aligned}$$

5 Infinite base fields

In this chapter we want to generalize Habegger's result. Before we state our theorem, we have to give a definition.

Definition 5.1
Let L be a Galois extension of $\mathbb{Q}$ and S a set of prime numbers. We say that L has *uniformly bounded local degrees* above S if and only if there exists $d \in \mathbb{N}$ such that for all primes $p \in S$ and v extending p, we have $[L_v : \mathbb{Q}_p] \leq d$. Here, L_v is the v-adic completion of L.

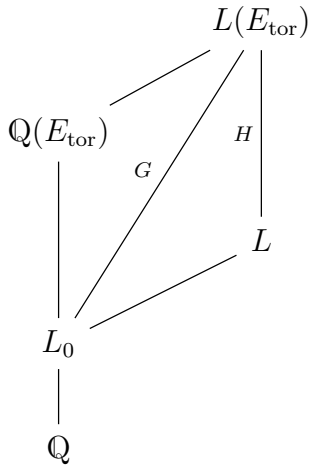
Our goal is proving the following theorem.

Theorem 5.2
Let E be an elliptic curve over $\mathbb{Q}$ and let $L/\mathbb{Q}$ be a Galois extension with uniformly bounded local degrees above all but finitely many primes. Then $L(E_{tor})$ has the Bogomolov property.

We will first prove the CM case since it follows from Theorem 1.5 of [ADZ14] before we handle the more complicated non-CM case.

Theorem 5.3
Let E be an elliptic curve with complex multiplication over $\mathbb{Q}$ and let $L/\mathbb{Q}$ be a Galois extension with uniformly bounded local degrees above all but finitely many primes. Then $L(E_{tor})$ has the Bogomolov property.

Proof
We consider the following diagram



Consider the restriction $f : G \to \mathrm{Gal}(\mathbb{Q}(E_{\mathrm{tor}})/L_0) \times \mathrm{Gal}(L/L_0), \sigma \mapsto (\sigma|_{\mathbb{Q}(E_{\mathrm{tor}})}, \sigma|_L)$. It is injective because $L(E_{\mathrm{tor}})$ is the compositum of L and $\mathbb{Q}(E_{\mathrm{tor}})$, hence the only element that maps to the identity is the identity itself.

We want to show that $\mathrm{Gal}(L(E_{\mathrm{tor}})/L) =: H$ is contained in the center of $\mathrm{Gal}(L(E_{\mathrm{tor}})/L_0) =: G$ since that will allow us to use Theorem 1.5 of [ADZ14] and immediately yield that $L(E_{\mathrm{tor}})$ is Bogomolov.

Let $\sigma \in G$ and $\tau \in H$. Then $\sigma\tau|_{\mathbb{Q}(E_{\mathrm{tor}})} = \tau\sigma|_{\mathbb{Q}(E_{\mathrm{tor}})}$ since G is abelian (because of E having complex multiplication). Furthermore $\sigma\tau|_L = \sigma|_L$ since τ acts as the identity on L and $\sigma|_L = \tau\sigma|_L$ since the image of σ is inside L (because L/L_0 is Galois). □

For the non-CM case we will make use of a result by Checcoli.

Theorem 5.4 ([Che13])
Let $L/\mathbb{Q}$ be a Galois extension. Then the following conditions are equivalent:

(1) L has uniformly bounded local degrees above every prime.

(2) L has uniformly bounded local degrees above all but finitely many primes.

(3) $\mathrm{Gal}(L/\mathbb{Q})$ has finite exponent.

Remark that uniformly bounded means that the degrees are bounded independently of p.

In a paper of Checcoli and Zannier [CZ11] there is also the implication (2) ⇒ (3) from the above theorem. But since we need the stronger implication (1) ⇒ (3), we use the result of Checcoli.

Example
A field that fulfills these properties is for a fixed d any subextension of $\mathbb{Q}^{(d)} \subset \overline{\mathbb{Q}}$, which is the compositum of all number fields of degree at most d over $\mathbb{Q}$.

5.1 Local preliminaries

For the rest of this chapter we will fix an elliptic curve E over $\mathbb{Q}$ without complex multiplication and with j-invariant j_E. Furthermore, fix a field L with the properties from Theorem 5.4 and call d the uniform bound for the local degrees. Then we will chose a prime p such that p fulfills properties (P1), (P2) and (P3) that we will define later. For $N \in \mathbb{N}$ we let $N = p^n M$ where M and p are coprime.

Recall also the notation $F(N) = F(E[N])$ for a field F and a natural number N.

We want to consider every field as a subfield of a fixed algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$. The proof goes as follows: For an element $\alpha \in L(E_{\mathrm{tor}})$ we will fix a finite Galois

extension $K/\mathbb{Q}$ such that $K(E_{\text{tor}})$ contains α and $K \subset L \subset \overline{\mathbb{Q}_p}$. Set $q = p^2$ and recall that $\mathbb{Q}_q$ denotes the unique quadratic unramified extension of $\mathbb{Q}_p$. Then we fix a Galois extension F of $\mathbb{Q}_q$ such that: $\mathbb{Q}_q \subset F \subset \overline{\mathbb{Q}_p}$, the v-adic completion of K is contained in F (where v extends p) and $[F : \mathbb{Q}_p]$ is uniformly bounded by $2d$ (since it is possible that we have to chose F larger than K_v so that it contains $\mathbb{Q}_q$). Since we consider all fields as subfields of $\overline{\mathbb{Q}_p}$ we can restrict the p-adic valuation of $\overline{\mathbb{Q}_p}$ to any subfield. Since all fields are Galois, the completion with respect to any place above p will be the same. We recall the properties we want p to have:

$$(P1) \quad p \text{ is supersingular} \tag{5.1}$$
$$(P2) \quad p \text{ is surjective} \tag{5.2}$$
$$(P3) \quad p \geq \max(2d+2, \exp(\mathrm{Gal}(L/\mathbb{Q}))) \tag{5.3}$$
$$(P4) \quad j_E \not\equiv 0, 1728 \bmod p \tag{5.4}$$

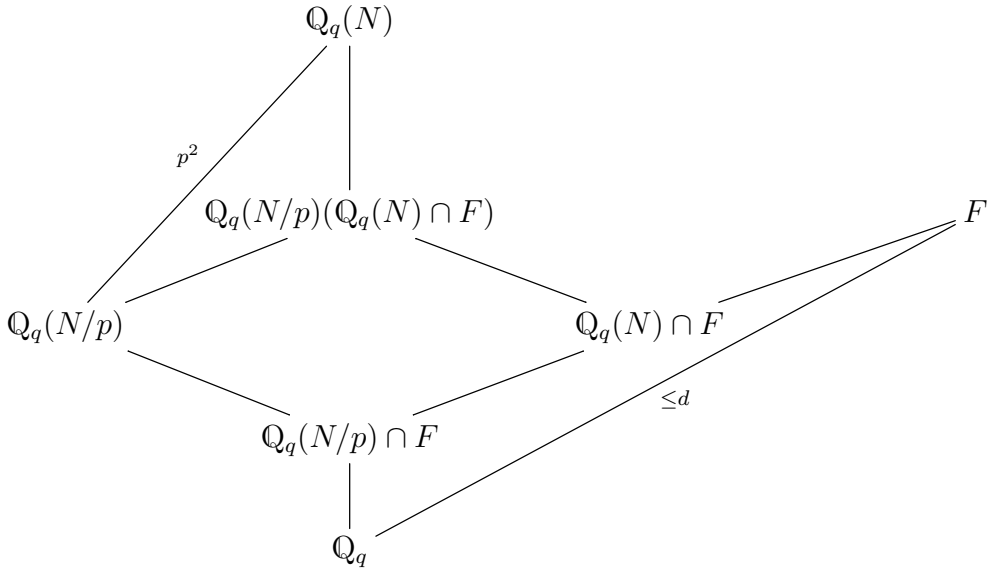
For a natural number N, we consider $F(N)$ and deal with two cases: the wildly ramified case where $p^2 \mid N$ and the tamely ramified case where $p^2 \nmid N$. We start with a few technical lemmas.

Lemma 5.5
Let $p^2|N$. We have $\mathbb{Q}_q(N) \cap F = \mathbb{Q}_q(N/p) \cap F$.

Proof
Recall that $p > d \geq [F : \mathbb{Q}_p]$. By Lemma 3.4 (v) of [Hab13] we know that

$$\mathrm{Gal}(\mathbb{Q}_q(N)/\mathbb{Q}_q(N/p)) \cong (\mathbb{Z}/p\mathbb{Z})^2$$

in the case of $p^2 \mid N$. We consider the following diagram where the numbers next to the lines describe the degrees of the extensions:



By the multiplicativity of the degree in a tower of field extensions, we have that

$$[\mathbb{Q}_q(N/p)(\mathbb{Q}_q(N) \cap F) : \mathbb{Q}_q(N/p)] \mid p^2$$

and by the above diagram

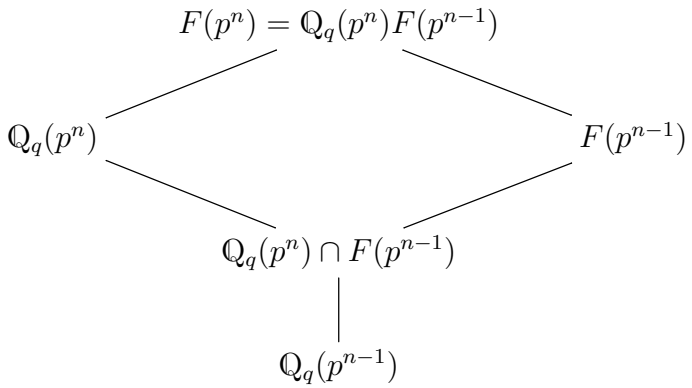
$$[\mathbb{Q}_q(N/p)(\mathbb{Q}_q(N) \cap F) : \mathbb{Q}_q(N/p)] = [\mathbb{Q}_q(N) \cap F : \mathbb{Q}_q(N/p) \cap F] \leq d < p.$$

Hence $[\mathbb{Q}_q(N) \cap F : \mathbb{Q}_q(N/p) \cap F]$ must be one and the fields are equal. $\square$

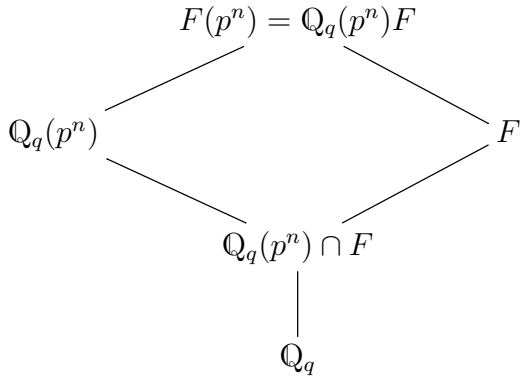
Lemma 5.6
Let $p^2 \mid N$. Then the extension $F(p^n)/F$ is abelian. Furthermore,

$$\mathrm{Gal}(F(p^n)/F(p^{n-1})) \cong (\mathbb{Z}/p\mathbb{Z})^2.$$

Proof
Consider the following diagram:



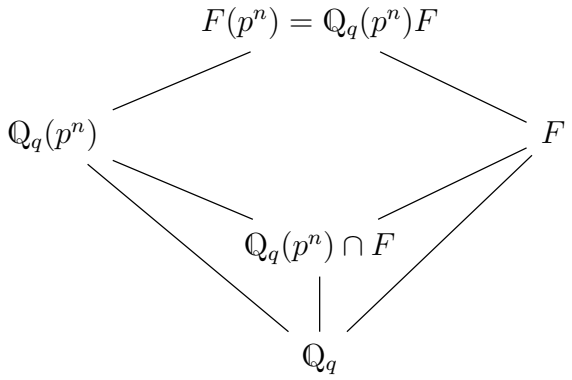
We get that $\mathrm{Gal}(F(p^n)/F(p^{n-1}))$ is isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q(p^{n-1}))$ of index at most $[F : \mathbb{Q}_q]$. Since by Lemma 3.4 (v) of [Hab13] $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q(p^{n-1}))$ has order p^2 and $[F : \mathbb{Q}_q]$ is strictly less than p, we must have $\mathrm{Gal}(F(p^n)/F(p^{n-1})) \cong \mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q(p^{n-1}))$. By Lemma 3.3 (i) of [Hab13], we get $\mathrm{Gal}(F(p^n)/F(p^{n-1})) \cong (\mathbb{Z}/p\mathbb{Z})^2$. To prove that $F(p^n)/F$ is abelian, we look at the following diagram



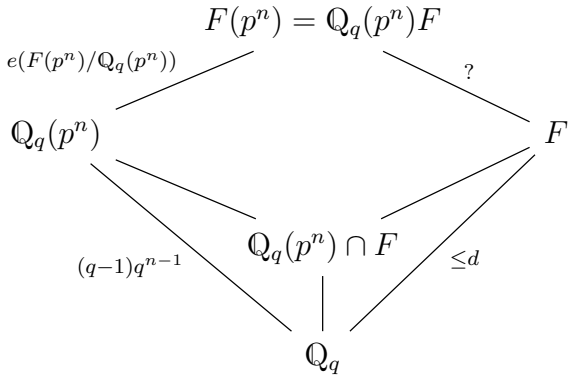
So by [Hab13], Lemma 3.4 (iv), $\mathrm{Gal}(F(p^n)/F)$ is isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q)$ which is isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z} \times (\mathbb{Z}/p^{n-1}\mathbb{Z})^2$, hence both Galois groups have to be abelian. □

Lemma 5.7
Let $p^2 \mid N$. The ramification index of the extension $F(p^n)/F$ is a multiple of q^{n-1} and a divisor of $q^{n-1}(q-1)$. The extension $F(p^n)/F(p^{n-1})$ is totally ramified and its Galois group is isomorphic to $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q(p^{n-1})) \cong (\mathbb{Z}/p\mathbb{Z})^2$. *In particular, $F(p^n)/F(p)$ is totally ramified.*

Proof
We consider the following diagram:



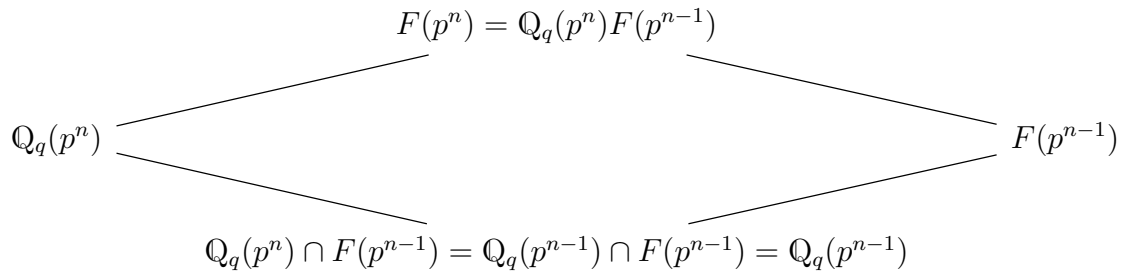
We want to equip this diagram with the ramification indices. From Lemma 3.3 (i) of [Hab13], we know that $\mathbb{Q}_q(p^n)/\mathbb{Q}_q$ is totally ramified of degree $(q-1)q^{n-1}$. By definition, the extension $F/\mathbb{Q}_q$ has degree (hence ramification index) at most d which is less than p. Since $\mathrm{Gal}(F(p^n)/\mathbb{Q}_q(p^n))$ is isomorphic to a subgroup of $\mathrm{Gal}(F/\mathbb{Q}_q)$, its degree has to be at most d hence also the ramification index. So we get the following diagram.



This shows that the ramification index of $F(p^n)/\mathbb{Q}_q$ is a multiple of the ramification degree of $\mathbb{Q}_q(p^n)/\mathbb{Q}_q$ which is $(q-1)q^{n-1}$. But since the ramification degree

of $F/\mathbb{Q}_q$ is at most d which is coprime to p, we get that the ramification degree of $F(p^n)/F$ has to be a multiple of q^{n-1}.

With a similar diagram we can show that $F(p^n)/F(p^{n-1})$ is totally ramified. Recall that by Lemma 5.5 we have $\mathbb{Q}_q(p^{n-1}) \cap F = \mathbb{Q}_q(p^n) \cap F$ and hence also $\mathbb{Q}_q(p^{n-1}) = \mathbb{Q}_q(p^n) \cap F(p^{n-1})$.



The ramification index of $\mathbb{Q}_q(p^n)/\mathbb{Q}_q(p^{n-1})$ is exactly q and the ramification index of $F(p^n)/\mathbb{Q}_q(p^n)$ is at most the degree $[F(p^n) : \mathbb{Q}_q(p^n)] \leq [F : \mathbb{Q}_q] < p$, hence not divisible by p. By looking at the divisibility we see that the ramification index of $F(p^n)/F(p^{n-1})$ also has to be q, hence it is totally ramified. Furthermore, $\mathrm{Gal}(F(p^n)/F(p^{n-1}))$ is isomorphic to $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q(p^{n-1}))$. □

The following lemma is the analogue of Lemma 3.4 of [Hab13].

Lemma 5.8
The following statements hold.

(i) *The compositum $F(p^n)F(M)$ is $F(N)$.*

(ii) *The extension $F(N)/F(p^n)$ is unramified.*

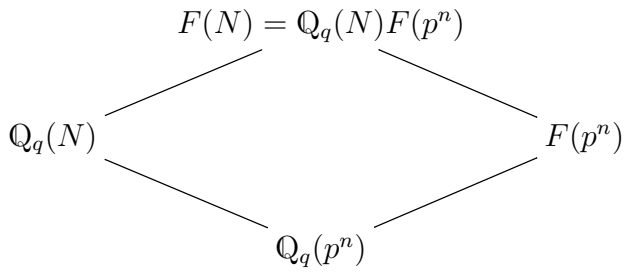
(iii) $\mathrm{Gal}(F(N)/F(M))$ *is abelian.*

(iv) *If $n \geq 2$, then $\mathrm{Gal}(F(N)/F(N/p)) \cong \mathrm{Gal}(F(p^n)/F(p^{n-1})) \cong (\mathbb{Z}/p\mathbb{Z})^2$ and the extension $F(N)/F(N/p)$ is totally ramified.*

(v) *The image of the representation $\mathrm{Gal}(F(p^n)/F) \to \mathrm{Aut}(E[p^n])$ contains multiplication by $M^{[F:\mathbb{Q}_q]}$.*

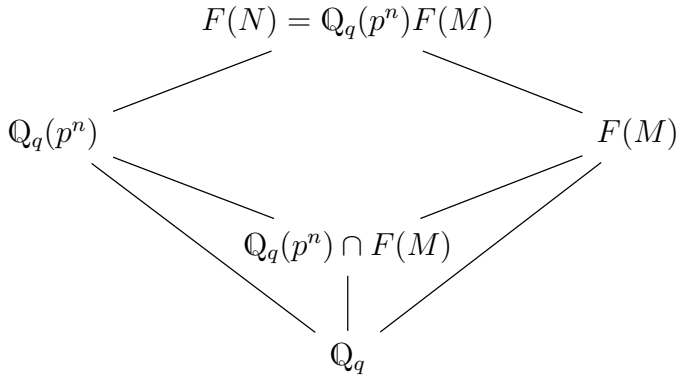
(vi) $\mathrm{Gal}(F(p)/F)$ *is isomorphic to a subgroup of $\mathbb{Z}/(q-1)\mathbb{Z}$.*

Proof
Every N-torsion point is the sum of a p^n-torsion point and an M-torsion point. Hence, the composition $F(p^n)F(M)$ has to be equal to $F(N)$ which is the statement in (i).
For (ii) we consider the following diagram:



Since the extension $\mathbb{Q}_q(N)/\mathbb{Q}_q(p^n)$ is unramified by Lemma 3.4 (ii) [Hab13], the subextension $\mathbb{Q}_q(N)/\mathbb{Q}_q(N) \cap F(p^n)$ also has to be unramified. Hence by [Neu99] Proposition 7.2, the extension $F(N)/F(p^n)$ extension also has to be unramified.

For (iii) we consider the following diagram:

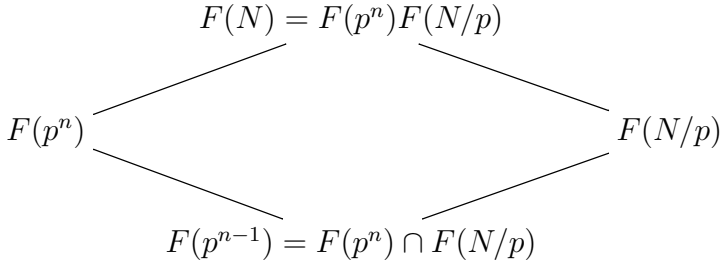


So $\mathrm{Gal}(F(N)/F(M))$ is a subgroup of $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q)$ which is by [Hab13], Lemma 3.4 (iv), isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z} \times (\mathbb{Z}/p^{n-1}\mathbb{Z})^2$, so it has to be abelian.

For (iv) we recall Lemma 3.4 (iv) of [Hab13]:

$$\mathrm{Gal}(\mathbb{Q}_q(N)/\mathbb{Q}_q(N/p)) \cong \begin{cases} (\mathbb{Z}/p\mathbb{Z})^2 & \text{if } n \geq 2, \\ \mathbb{Z}/(q-1)\mathbb{Z} & \text{if } n = 1. \end{cases}$$

Let now $n \geq 2$. We want to use Lemma 2.1 (i) of [Hab13] with the unramified extension $F(N/p)/F(p^{n-1})$ (see Lemma 5.8 (ii)) and the totally ramified extension $F(p^n)/F(p^{n-1})$ (see Lemma 5.7). We get $F(p^{n-1}) = F(p^n) \cap F(N/p)$ and with the following diagram



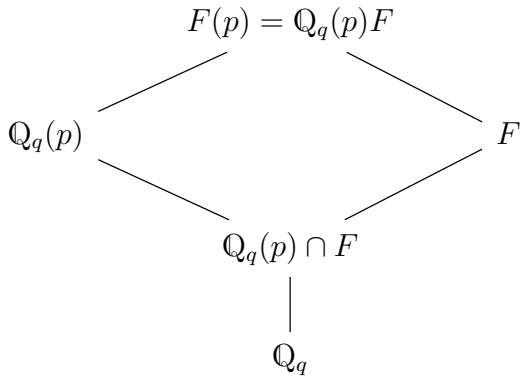
we can use Lemma 5.6 and get

$$\mathrm{Gal}(F(N)/F(N/p)) \cong \mathrm{Gal}(F(p^n)/F(p^{n-1})) \cong (\mathbb{Z}/p\mathbb{Z})^2.$$

With Lemma (ii) 2.1 of [Hab13], we get that the extension $F(N)/F(N/p)$ is totally ramified.

We now come to part (v). By Lemma 3.3 (iii) of [Hab13], the image of the representation $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q) \to \mathrm{Aut}(E[p^n])$ contains multiplication by M. Let us call σ the preimage of multiplication by M. By restriction we get a representation $\mathrm{Gal}(F(p^n)/\mathbb{Q}_q) \to \mathrm{Aut}(E[p^n])$ that is compatible to the above one and we can choose an element in $\mathrm{Gal}(F(p^n)/\mathbb{Q}_q)$ that restricts to σ in $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q)$. We will call this element also σ. Since $\mathrm{Gal}(F(p^n)/F)$ is a normal subgroup of $\mathrm{Gal}(F(p^n)/\mathbb{Q}_q)$, we can look at the projection $f : \mathrm{Gal}(F(p^n)/\mathbb{Q}_q) \to \mathrm{Gal}(F(p^n)/\mathbb{Q}_q)/\mathrm{Gal}(F(p^n)/F)$. The index of $\mathrm{Gal}(F(p^n)/\mathbb{Q}_q)$ in $\mathrm{Gal}(F(p^n)/F)$ is equal to $[F : \mathbb{Q}_q]$. So $f(\sigma^{[F:\mathbb{Q}_q]}) = f(\sigma)^{[F:\mathbb{Q}_q]} = id$. Hence $\sigma^{[F:\mathbb{Q}_q]}$ is an element of $\mathrm{Gal}(F(p^n)/F)$ and it will act as multiplication by $M^{[F:\mathbb{Q}_q]}$.

For (vi) we consider the following diagram.



By [Hab13], Lemma 3.4 (iv), we know that $\mathrm{Gal}(\mathbb{Q}_q(p)/\mathbb{Q}_q) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. So $\mathrm{Gal}(F(p)/F)$ has to be isomorphic to a subgroup of $\mathbb{Z}/(q-1)\mathbb{Z}$. □

Recall the definition of the higher ramification groups.

$$G_i(L/K) := \{\sigma \in \mathrm{Gal}(L/K) | \forall a \in \mathcal{O}_K \text{ we have } w(\sigma(a) - a) \geq i + 1\}.$$

Lemma 5.9
Let $p^2 \mid N$. Then there is $s \geq q^{n-1} - 1$ such that

$$\mathrm{Gal}(F(N)/F(N/p)) \subset G_s(F(N)/F).$$

Proof
First, we want to show that $\mathrm{Gal}(F(p^n)/F(p^{n-1})) \subset G_s(F(p^n)/\mathbb{Q}_q)$ for some $s \geq q^{n-1} - 1$.

By Lemma 3.3 (ii) of [Hab13], we know that $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q(p^{n-1})) = G_{q^{n-1}-1}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q)$. So we take an element ψ of $\mathrm{Gal}(F(p^n)/F(p^{n-1}))$ and look at the restriction to $\mathbb{Q}_q(p^n)$ which will be an element of $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q(p^{n-1}))$ and hence of $G_{q^{n-1}-1}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q)$. We will use Herbrand's Theorem (Theorem 10.7 of [Neu99]) which says that for any $s \geq -1$

$$(G_s(F(p^n)/\mathbb{Q}_q)\,\mathrm{Gal}(F(p^n)/\mathbb{Q}_q(p^n)))/\,\mathrm{Gal}(F(p^n)/\mathbb{Q}_q(p^n)) = G_t(\mathbb{Q}_q(p^n)/\mathbb{Q}_q)$$

where t depends on s. By Proposition IV.12 of [Ser79] t is given by a continuous and increasing function of s that maps 0 to 0 and goes to infinity as s goes to infinity. By the piecewise linearity seen in the equation on p. 73 of [Ser79], we see that for $t = q^{n-1} - 1$ we can find s such that the above is true and $s \geq t$.

Now since the restriction $\psi|_{\mathbb{Q}_q(p^n)}$ is an element of $G_{q^{n-1}-1}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q)$ we find $\sigma_1 \in G_s(F(p^n)/\mathbb{Q}_q)$ and $\sigma_2 \in \mathrm{Gal}(F(p^n)/\mathbb{Q}_q(p^n))$ such that $\psi = \sigma_1\sigma_2$. Since $G_s(F(p^n)/\mathbb{Q}_q)$ is a normal subgroup of $\mathrm{Gal}(F(p^n)/\mathbb{Q}_q)$, we can consider $\mathrm{Gal}(F(p^n)/\mathbb{Q}_q)/G_s(F(p^n)/\mathbb{Q}_q)$. We want to consider the homomorphism of groups

$$f : \mathrm{Gal}(F(p^n)/\mathbb{Q}_q) \to \mathrm{Gal}(F(p^n)/\mathbb{Q}_q)/G_s(F(p^n)/\mathbb{Q}_q).$$

Since $\sigma_1 \in G_s(F(p^n)/\mathbb{Q}_q)$ we have $f(\sigma_1) = \mathrm{id}$. Furthermore,

$$\begin{aligned} f(\sigma_1\sigma_2)^{[F(p^n):\mathbb{Q}_q(p^n)]} &= (f(\sigma_1)f(\sigma_2))^{[F(p^n):\mathbb{Q}_q(p^n)]} \\ &= f(\sigma_2)^{[F(p^n):\mathbb{Q}_q(p^n)]} \\ &= f((\sigma_2)^{[F(p^n):\mathbb{Q}_q(p^n)]}) \\ &= f(\mathrm{id}) \\ &= \mathrm{id}\,. \end{aligned}$$

So with $e := [F : \mathbb{Q}_q]!$ we can make sure that $(\sigma_1\sigma_2)^e \in G_s(F(p^n)/\mathbb{Q}_q)$. But since ψ was in $\mathrm{Gal}(F(p^n)/F(p^{n-1}))$ which is by Lemma 5.8 (iv) isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$ and e is coprime to the order of $\mathrm{Gal}(F(p^n)/F(p^{n-1}))$, we can find $\tilde{\psi} \in \mathrm{Gal}(F(p^n)/F(p^{n-1}))$ such that $\tilde{\psi}^e = \psi$.

Hence we get that

$$\mathrm{Gal}(F(p^n)/F(p^{n-1})) \subset G_s(F(p^n)/\mathbb{Q}_q) = G \tag{5.5}$$

and we showed that there exists $s \geq q^{n-1} - 1$ such that $G_s(F(p^n)/\mathbb{Q}_q)$ has order p^2.

Now by Lemma 2.1 (iii) of [Hab13] and with $F(N/p)/F(p^{n-1})$ unramified and $F(p^n)/F(p^{n-1})$ totally ramified, we have

$$\mathrm{Gal}(F(N)/F(N/p)) \cap G_s(F(N)/F(p^{n-1})) \cong G_s(F(p^n)/F(p^{n-1})) \tag{5.6}$$

by restriction. By Lemma 5.8 (iv), $\mathrm{Gal}(F(N)/F(N/p))$ must have order p^2 and since $G_s(F(p^n)/F(p^{n-1}))$ also has order p^2, they have to be isomorphic by restriction. By set theory, we then get

$$\begin{aligned}\mathrm{Gal}(F(N)/F(N/p)) &= \mathrm{Gal}(F(N)/F(N/p)) \cap G_s(F(N)/F(p^{n-1})) \\ &\subset G_s(F(N)/F(p^{n-1})). \end{aligned} \tag{5.7}$$

By the formal definition of the higher ramification group we get that

$$G_s(F(N)/F(p^{n-1})) \cong G_s(F(N)/F) \cap \mathrm{Gal}(F(N)/F(p^{n-1})) \subset G_s(F(N)/F).$$

Hence $\mathrm{Gal}(F(N)/F(N/p))$ is isomorphic to a subgroup of $G_s(F(N)/F)$ which is what we wanted to show. □

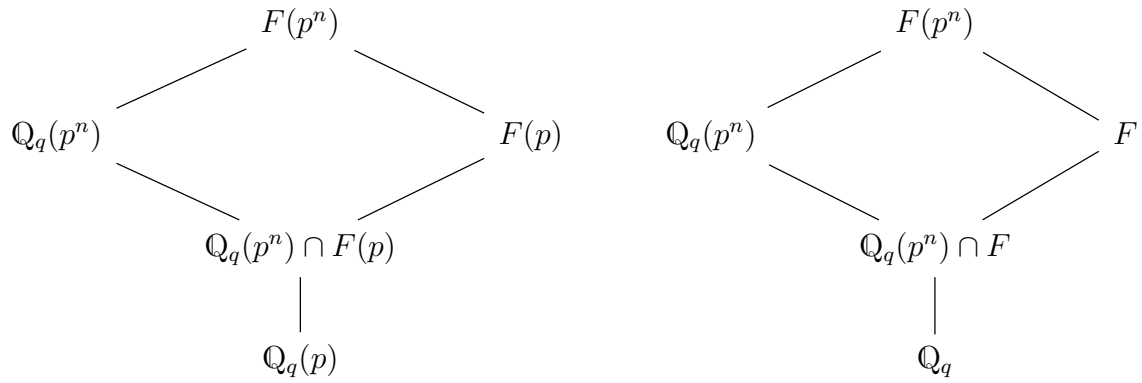
Lemma 5.10
Let $n \geq 2$. We have $F(N) \cap \mu_{p^\infty} = \mu_{p^n}$.

Proof
Since by Lemma 3.5 of [Hab13] $\mathbb{Q}_q(N) \cap \mu_{p^\infty} = \mu_{p^n}$, we have $F(N) \supset \mu_{p^n}$ and we only have to show "$\subset$". We will closely follow Habegger's proof of Lemma 3.5 of [Hab13] and first show that $F(p^n) \cap \mu_{p^\infty} = \mu_{p^n}$. Let $\zeta \in F(p^n)$ be a root of unity of order $p^{n'}$ with $n' \geq n$. By restricting we get a surjective homomorphism

$$\mathrm{Gal}(F(p^n)/F) \twoheadrightarrow \mathrm{Gal}(F(\zeta)/F).$$

We will later prove that the left group is isomorphic to $(\mathbb{Z}/p^{n-1}\mathbb{Z})^2 \times A$ where A is a subgroup of $\mathbb{Z}/(q-1)\mathbb{Z}$. The right part is isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ which itself is isomorphic to $\mathbb{Z}/p^{n'-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$ by Proposition II.7.13 of [Neu99]. Remark that $\mathbb{Z}/p^{n'-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$ is cyclic since $p-1$ and p are coprime, hence all subgroups are direct products of subgroups. Since the index of $\mathrm{Gal}(F(\zeta)/F)$ in $\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ can be at most $[F : \mathbb{Q}_p]$ which is less than p, we must have that $\mathrm{Gal}(F(\zeta)/F)$ is actually isomorphic to $\mathbb{Z}/p^{n'-1}\mathbb{Z} \times A$ where A is a subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$. Recall that $\mathrm{Gal}\, F(p^n)/F)$ is isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{Q}_q(p^n)/\mathbb{Q}_q) \cong (\mathbb{Z}/p^{n-1}\mathbb{Z})^2 \times \mathbb{Z}/(p-1)\mathbb{Z}$. So the homomorphism can only be surjective if it maps $(\mathbb{Z}/p^{n-1}\mathbb{Z})^2$ surjectively to $\mathbb{Z}/p^{n'-1}\mathbb{Z}$ which is only possible when $n \geq n'$. Together with $n' \geq n$ we get that $n' = n$. Let now $\zeta \in F(N)$ be a root of unity of order $p^{n'}$ with $n' \geq n$. The extension $F(N)/F(p^n)$ is unramified, hence also $F(p^n)(\zeta)/F(p^n)$. By the properties of the Weil pairing we know that $\zeta \in \mathbb{Q}_p(p^{n'}) \subset F(p^{n'})$. By Lemma 5.7, the extension $F(p^{n'})/F(p^n)$ is totally ramified and so is $F(p^n)(\zeta)/F(p^n)$. Hence this extension must be trivial and we have $\zeta \in F(p^n)$.

So let us now prove that $\mathrm{Gal}(F(p^n)/F) \cong (\mathbb{Z}/p^{n-1}\mathbb{Z})^2 \times A$. Recall that p and $[F : \mathbb{Q}_q]$ are coprime and consider the following diagrams:



The diagram on the right hand side shows that $\mathrm{Gal}(F(p^n)/F)$ is isomorphic to a subgroup $(\mathbb{Z}/p^{n-1}\mathbb{Z})^2 \times \mathbb{Z}/(q-1)\mathbb{Z}$. The diagram on the left hand side shows that $\mathrm{Gal}(F(p^n)/F(p))$ is isomorphic to a subgoup of $(\mathbb{Z}/p^{n-1}\mathbb{Z})^2$. By Goursat's Lemma [Gou89] and since their orders are equal, the groups have to be isomorphic. □

Lemma 5.11
Let $\psi \in \mathrm{Gal}(F(N)/F(N/p))$ and $\xi \in F(N) \cap \mu_{M'}$. Then $\psi(\xi) = \xi$.

Proof
By Proposition II 7.12 of [Neu99], the extension $F(\xi)/F$ is unramified.

Now we want to prove that $F(\xi) \subset F(N/p)$ (and hence $\psi(\xi) = \xi$). We know that $F(\xi)/F$ is unramified, hence $F(N/p)(\xi)/F(N/p)$ is also unramified. Furthermore, by Lemma 5.8 (iv), $F(N)/F(N/p)$ is totally ramified, hence as a subextension, $F(N/p)(\xi)/F(N/p)$ also has to be totally ramified. But totally ramified and unramified extensions are trivial and we get that $F(N/p)(\xi) = F(N/p)$, hence $F(\xi) \subset F(N/p)$. □

Lemma 5.12
Let $N = p^n M$ with $n \geq 2$. If $\psi \in \mathrm{Gal}(F(N)/F(N/p))$ and $\alpha \in F(N) \setminus \{0\}$ such that $\frac{\psi(\alpha)}{\alpha} \in \mu_\infty$, then

$$\frac{\psi(\alpha)}{\alpha} \in \mu_q. \tag{5.8}$$

Proof
We will follow the analogous proof of Lemma 3.6 in [Hab13] very closely and only change it where we need to use generalized results of this section.

We write x^ψ for $\psi(x)$ if $x \in F(N)$, hence $\frac{\psi(\alpha)}{\alpha} = \alpha^{\psi-1}$. Let N' denote the order of $\beta := \alpha^{\psi-1}$ and decompose it as $N' = p^{n'}M'$ with nonnegative n' and M' and p coprime. Then $\xi := \beta^{p^{n'}}$ has order M'. By the lemma above, ξ is fixed by ψ.

The order of $\beta^{M'}$ is $p^{n'}$. Hence $n' \leq n$ by the above Lemma 5.10. For the same reason we have $\beta^{pM'} \in F(N/p)$, hence ψ fixes $\beta^{pM'}$.

Let us write $1 = ap^{n'} + bM'$ with a and b integers. Then $\beta = \xi^a \beta^{bM'}$ and so ψ fixes β^p since it fixes ξ and $\beta^{pM'}$.

Let t denote the order of ψ as an element of $\mathrm{Gal}(F(N)/F(N/p))$. Then

$$1 = \alpha^{p(\psi^t-1)} = \alpha^{p(\psi-1)(\psi^{t-1}+\ldots+\psi+1)} = \beta^{p(\psi^{t-1}+\ldots+\psi+1)} = \beta^{pt}. \tag{5.9}$$

By Lemma 5.8 (iv) the order t divides p and the statement follows. □

5.2 The tamely ramified case

Again, we fix E, L and p as in section 5.1.

Remark that the tamely ramified case includes the unramified case. For the whole section let $p^2 \nmid N$ and $\varphi_q \in \mathrm{Gal}(\mathbb{Q}_q^{\mathrm{unr}}/\mathbb{Q}_q)$ be the lift of the Frobenius squared as in [Hab13]. For $p \nmid N$ we let $\tilde{F} := F$ and for $p \mid N$ we let $\tilde{F} := F(p)$. Recall that the extension $F/\mathbb{Q}_q$ is Galois.

Lemma 5.13
Let $\mathcal{E}$ be a multiple of $[F : \mathbb{Q}_q](q-1)$. We have

(i) $\varphi_q^{\mathcal{E}}|_{\tilde{F}\cap\mathbb{Q}_q^{unr}} = \mathrm{id}$.

(ii) There exists $\tilde{\varphi}$ in $\mathrm{Gal}(\tilde{F}(M)/\tilde{F})$ such that the restriction $\tilde{\varphi}|_{(\tilde{F}\cap\mathbb{Q}_q^{unr})(M)}$ coincides with the restriction $\varphi_q^{\mathcal{E}}|_{(\tilde{F}\cap\mathbb{Q}_q^{unr})(M)}$.

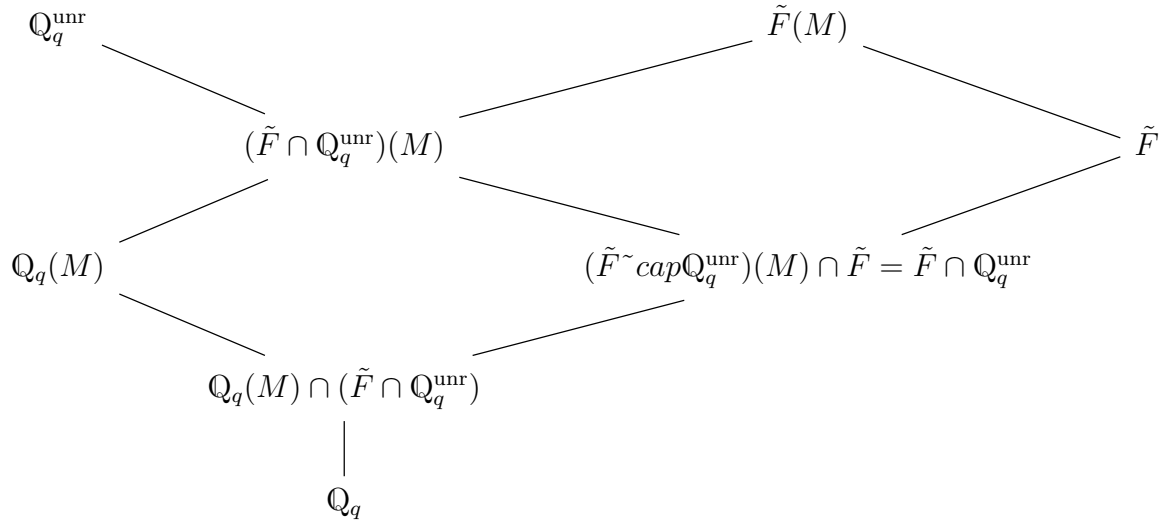
(iii) For $\tilde{\varphi}$ from (ii) we have that $\tilde{\varphi}|_{K(N)}$ lies in the center of $\mathrm{Gal}(K(N)/\mathbb{Q})$.

(iv) The extension $\tilde{F}(M)/(\tilde{F}\cap\mathbb{Q}_q^{unr})(M)$ is totally ramified.

(v) The ramification index of $\tilde{F}(M)/\mathbb{Q}_q$ is at most $(q-1)[F:\mathbb{Q}_q] \leq \mathcal{E}$.

Proof
(i) We have that $[F : \mathbb{Q}_p]$ is a multiple of $|\mathrm{Gal}(\mathcal{O}_F/\mathfrak{P}/\mathcal{O}_{\mathbb{Q}_q}/\mathfrak{p})|$ where $\mathfrak{P}$ and $\mathfrak{p}$ are the maximal ideals of $\mathcal{O}_F$ and $\mathcal{O}_{\mathbb{Q}_q}$, respectively. By Lemma 5.8 (vi) we have that $\mathrm{Gal}(F(p)/F) \subset \mathbb{Z}/(q-1)\mathbb{Z}$ hence in the case of $p|N$ we have that $[\tilde{F} : \mathbb{Q}_q]$ is a divisor of $[F : \mathbb{Q}_q](q-1)$ which divides $\mathcal{E}$ and whenever $p \nmid N$, we still have that $[\tilde{F} : \mathbb{Q}_q]|\mathcal{E}$. So $\mathcal{E}$ is always a multiple of the local degree $[\tilde{F} : \mathbb{Q}_q]$. Since $\varphi_q|_{\tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}}}$ acts trivially on $\mathcal{O}_{\mathbb{Q}_q}/\mathfrak{p}$, it is an element of the Galois group $\mathrm{Gal}(\tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}}/\mathbb{Q}_q)$. But the order of this group is a divisor of $\mathcal{E}$ since $\mathrm{Gal}(\tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}}/\mathbb{Q}_q)$ is a quotient of $\mathrm{Gal}(\tilde{F}/\mathbb{Q}_q)$ which has order dividing $(q-1)[F : \mathbb{Q}_q]$. Hence, its $\mathcal{E}$-th power has to be the identity.

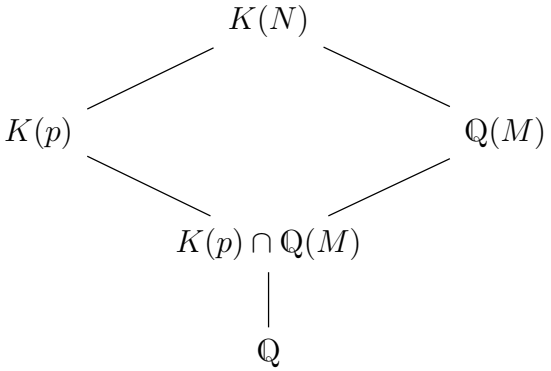
(ii) First, we want to show that $(\tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}})(M)\cap\tilde{F} = \tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}}$. The inclusion $(\tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}})(M)\cap\tilde{F} \supset \tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}}$ is obvious and we have to prove "$\subset$". By Lemma 3.1 of [Hab13], the extension $\mathbb{Q}_q(M)/\mathbb{Q}_q$ is unramified, hence $\mathbb{Q}_q^{\mathrm{unr}}(M) = \mathbb{Q}_q^{\mathrm{unr}}$. We have $(\tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}})(M)\cap\tilde{F} \subset \mathbb{Q}_q^{\mathrm{unr}}(M)\cap\tilde{F} = \mathbb{Q}_q^{\mathrm{unr}}\cap\tilde{F}$.
We consider the following diagram:



Recall that $\mathcal{E}$ is a multiple of $(q-1)[F:\mathbb{Q}_p]$ and by (i) $\varphi_q^{\mathcal{E}}|_{\tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}}}$ is trivial. Hence $\varphi_q^{\mathcal{E}} \in \mathrm{Gal}(\mathbb{Q}_q^{\mathrm{unr}}/\tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}})$. By the diagram, the Galois group $\mathrm{Gal}((\tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}})(M)/\tilde{F}\cap\mathbb{Q}_q^{\mathrm{unr}})$ is isomorphic to $\mathrm{Gal}(\tilde{F}(M)/\tilde{F})$ and we call $\tilde{\varphi}$ the image under that isomorphism. Note that in the case of $p \mid N$, $\tilde{\varphi}$ acts trivially on $\tilde{F} = F(p) \supset K(p)$. In the case of $p \nmid N$, $\tilde{\varphi}$ acts trivially on $F \supset K$.

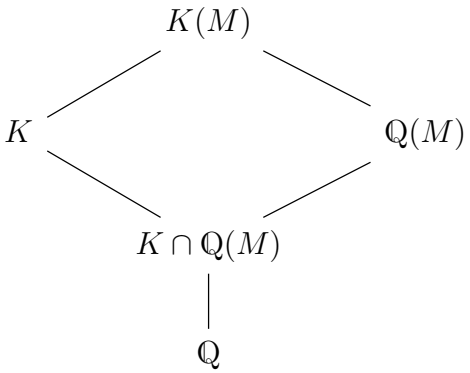
(iii) We will distinguish the two cases $p \nmid N$ and $p|N$.

For $p|N$ we already remarked that $\tilde{\varphi}|_{K(p)}$ is the identity and we now want to show that $\tilde{\varphi}|_{K(N)}$ lies in the center of $\mathrm{Gal}(K(N)/\mathbb{Q})$. Consider the following diagram



which shows that $\mathrm{Gal}(K(N)/\mathbb{Q})$ is by restriction isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{Q}(M)/\mathbb{Q}) \times \mathrm{Gal}(K(p)/\mathbb{Q})$. Now the proof of Lemma 5.1 of [Hab13] shows that $\tilde{\varphi}$ lies in the center of $\mathrm{Gal}(\mathbb{Q}(M)/\mathbb{Q})$. Together with $\tilde{\varphi}$ acting trivially on $K(p)$, we get that it lies in the center of $\mathrm{Gal}(K(N)/\mathbb{Q})$.

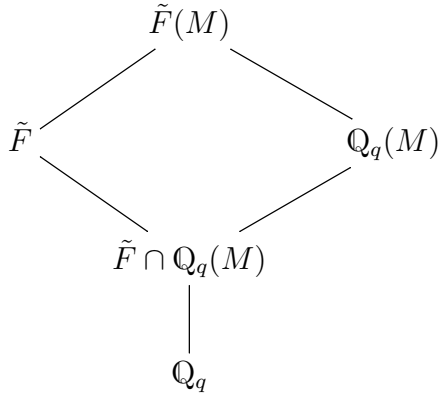
Now let $p \nmid N$. We do the same as above, considering K instead of $K(p)$. Consider the diagram:



And again: $\mathrm{Gal}(K(M)/\mathbb{Q})$ is by restriction isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{Q}(M)/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$ and since $\tilde{\varphi}$ acts trivially on K and lies in the center of $\mathrm{Gal}(\mathbb{Q}(M)/\mathbb{Q})$, it also lies in the center of $\mathrm{Gal}(K(M)/\mathbb{Q})$.

(iv) We will use Lemma 2.1 (ii) of [Hab13] again. Since $\tilde{F}/\tilde{F} \cap \mathbb{Q}_p^{\mathrm{unr}}$ is totally ramified and $(\tilde{F} \cap \mathbb{Q}_p^{\mathrm{unr}})(M)/\tilde{F} \cap \mathbb{Q}_p^{\mathrm{unr}}$ is unramified, the extension $\tilde{F}(M)/(\tilde{F} \cap \mathbb{Q}_p^{\mathrm{unr}})(M)$ is also totally ramified.

(v) We consider the following diagram



Since the extension $\mathbb{Q}_q(M)/\mathbb{Q}_q$ is unramified, the only contribution to the ramification degree can come from the extension $\tilde{F}(M)/\mathbb{Q}_q(M)$. Since the Galois group of the said extension is a subgroup of $\mathrm{Gal}(\tilde{F}/\mathbb{Q}_q)$, it has degree at most $(q-1)[F : \mathbb{Q}_q]$, hence also the ramification degree cannot be larger.

□

Lemma 5.14
Let L/K be a totally ramified extension of fields with $K \subset L \subset \overline{\mathbb{Q}_p}$ and $[L : \mathbb{Q}_p]$, $[K : \mathbb{Q}_p]$ finite. Then for every $\alpha \in \mathcal{O}_L$ there exists $\beta \in \mathcal{O}_K$ such that $|\alpha - \beta|_p < 1$.

Proof
Since the field extension is totally ramified, the residue fields are equal. Consider α as an element in the residue field of L. Take any $\beta \in \mathcal{O}_K$ in the same residue class

as α. Then, as α and β are in the same residue class, their difference $\alpha - \beta$ is zero in the residue field. This means $\alpha - \beta$ is an element of the maximal ideal, hence $|\alpha - \beta|_p$ has to be smaller than one. $\square$

Lemma 5.15
Let $\alpha \in \tilde{F}(M)^*$ with $|\alpha|_p \leq 1$. Then for $\tilde{\varphi}$ and $\mathcal{E}$ as in Lemma 5.13 we have

$$|\tilde{\varphi}(\alpha) - \alpha^{q^{\mathcal{E}}}|_p \leq p^{-\frac{1}{\mathcal{E}}}.$$

Proof
Let $\alpha \in \tilde{F}(M)$ with $|\alpha|_p \leq 1$. Then by Lemma 5.14 and 5.13 (iv) we find $\beta \in (\tilde{F} \cap \mathbb{Q}_q^{\mathrm{unr}})(M)$ with $|\beta|_p \leq 1$ and $|\alpha - \beta|_p < 1$. Now $|\tilde{\varphi}(\alpha) - \tilde{\varphi}(\beta)|_p = |\alpha - \beta|_p$ since Galois automorphisms do not change the valuation. Furthermore, we have

$$(\alpha^{q^{\mathcal{E}}} - \beta^{q^{\mathcal{E}}}) = (\alpha - \beta)(\alpha^{q^{\mathcal{E}}-1} + \alpha^{q^{[F:\mathbb{Q}_q]}-2}\beta + ... + \alpha\beta^{q^{[F:\mathbb{Q}_q]}-2} + \alpha^{q^{[F:\mathbb{Q}_q]}-1})$$

hence

$$\begin{aligned}
|\alpha^{q^{[F:\mathbb{Q}_q]}} - \beta^{q^{[F:\mathbb{Q}_q]}}|_p &= |\alpha - \beta|_p |\alpha^{q^{\mathcal{E}}-1} + \alpha^{q^{\mathcal{E}}-2}\beta + ... + \alpha\beta^{q^{\mathcal{E}}-2} + \alpha^{q^{\mathcal{E}}-1}|_p \\
&\leq |\alpha - \beta|_p \max(|\alpha^{q^{\mathcal{E}}-1}|_p, |\alpha^{q^{\mathcal{E}}-2}\beta|_p, ..., |\alpha\beta^{q^{\mathcal{E}}-2}|_p, |\alpha^{q^{\mathcal{E}}-1}|_p) \\
&\leq |\alpha - \beta|_p \\
&< 1.
\end{aligned}$$

Now consider $|\tilde{\varphi}(\beta) - \beta^{q^{\mathcal{E}}}|_p$. Since $\beta \in (\tilde{F} \cap \mathbb{Q}_q^{\mathrm{unr}})(M)$, we can apply Lemma 5.13 (ii) and get that $\tilde{\varphi}$ acts as $\tilde{\varphi}(\beta)$ is equal to $\beta^{q^{\mathcal{E}}}$ in the residue field. Again, as in the proof of the above lemma, this means that their difference is an element of the maximal ideal in $(\tilde{F} \cap \mathbb{Q}_q^{\mathrm{unr}})(M)$, which means that $|\tilde{\varphi}(\beta) - \beta^{q^{\mathcal{E}}}|_p < 1$.

So we have

$$\begin{aligned}
|\tilde{\varphi}(\alpha) - \alpha^{q^{\mathcal{E}}}|_p &= |\tilde{\varphi}(\alpha) - \tilde{\varphi}(\beta) + \tilde{\varphi}(\beta) - \beta^{q^{\mathcal{E}}} + \beta^{q^{\mathcal{E}}} - \alpha^{q^{\mathcal{E}}}|_p \\
&\leq \max(|\tilde{\varphi}(\alpha) - \tilde{\varphi}(\beta)|_p, |\tilde{\varphi}(\beta) - \beta^{q^{\mathcal{E}}}|_p, |\beta^{q^{\mathcal{E}}} - \alpha^{q^{\mathcal{E}}}|_p) \\
&= \max(|\alpha - \beta|_p, |\tilde{\varphi}(\beta) - \beta^{q^{\mathcal{E}}}|_p) \\
&< 1.
\end{aligned}$$

Since the valuation is discrete and we bounded the ramification degree in 5.13 (v), it has to be at most $p^{-\frac{1}{\mathcal{E}}}$ which proves the statement. $\square$

Lemma 5.16
Let $\alpha \in \tilde{F}(M)^*$. Then for $\tilde{\varphi}$ as in Lemma 5.13 we have

$$|\tilde{\varphi}(\alpha) - \alpha^{q^{\mathcal{E}}}|_p \leq p^{-\frac{1}{\mathcal{E}}}.$$

$$|\tilde{\varphi}(\alpha) - \alpha^{q^{\mathcal{E}}}|_p \leq p^{-\frac{1}{\mathcal{E}}} \max(1, |\tilde{\varphi}(\alpha)|_p) \max(1, |\alpha|_p)^{q^{\mathcal{E}}}.$$

Proof
For $|\alpha|_p \leq 1$ this is the above lemma. Let now $|\alpha|_p > 1$ and consider α^{-1}. Then we can use the ultrametric triangle inequality and with the above lemma we get

$$|\alpha^{-q^{\mathcal{E}}}(\tilde{\varphi}(\alpha) - \alpha^{q^{\mathcal{E}}})|_p = |(\alpha^{-q^{\mathcal{E}}} - \tilde{\varphi}(\alpha^{-1}))\tilde{\varphi}(\alpha)|_p \leq p^{-\frac{1}{\tilde{e}}}|\tilde{\varphi}(\alpha)|_p$$

which gives the desired result. □

Recall that an element $\sigma \in \mathrm{Gal}(K(N)/\mathbb{Q})$ acts on the places of $K(N)$ by $|\cdot|_{\sigma v} = |\sigma^{-1}(\cdot)|_v$.

Lemma 5.17
Let $p^2 \nmid N$. Let $\alpha \in K(N)\backslash\mu_\infty$ be non-zero. Then

$$h(\alpha) \geq \left(\frac{\log p}{\mathcal{E}(1+q^{\mathcal{E}})(1+5\cdot 2^{11})}\right)^4. \tag{5.10}$$

Proof
We follow the proof of Lemma 5.1 of [Hab13] closely. Let $x = \tilde{\varphi}|_{K(N)}(\alpha) - \alpha^{q^{\mathcal{E}}} \in K(N)$ where $\tilde{\varphi}|_{K(N)}$ is the lift of the Frobenius from before. This is nonzero since otherwise we would get $h(\alpha) = h(\tilde{\varphi}|_{K(N)}(\alpha)) = h(\alpha^{q^{\mathcal{E}}}) = q^{\mathcal{E}}h(\alpha)$ hence $h(\alpha) = 0$ which contradicts our assumption on α. So we can use the product formula

$$\sum_w d_w \log|x|_w = 0 \tag{5.11}$$

where the sum is over all places of $K(N)$.

Let w be a finite place of $K(N)$ above p. Then $w = \sigma^{-1}v$ for some $\sigma \in \mathrm{Gal}(K(N)/\mathbb{Q})$ and v a place above p because this Galois group acts transitively on the places of $K(N)$ above p. By Lemma 5.13 (iii) $\tilde{\varphi}|_{K(N)}$ and σ commute and we get

$$|x|_w = |\sigma(\tilde{\varphi}|_{K(N)}(\alpha)) - \sigma(\alpha)^{q^{\mathcal{E}}}|_v = |\tilde{\varphi}|_{K(N)}(\sigma(\alpha)) - \sigma(\alpha)^{q^{\mathcal{E}}}|_v.$$

Now we estimate the right-hand side from above using Lemma 5.16 applied to $\sigma(\alpha)$

$$\begin{aligned}|x|_w &\leq p^{-\frac{1}{\tilde{e}}}\max(1, |\tilde{\varphi}|_{K(N)}(\sigma(\alpha))|_v)\max(1, |\sigma(\alpha)|_v)^{q^{\mathcal{E}}} \\ &= p^{-\frac{1}{\tilde{e}}}\max(1, |\sigma(\tilde{\varphi}|_{K(N)}(\alpha))|_v)\max(1, |\sigma(\alpha)|_v)^{q^{\mathcal{E}}} \\ &= p^{-\frac{1}{\tilde{e}}}\max(1, |\tilde{\varphi}|_{K(N)}(\alpha)|_w)\max(1, |\alpha|_w)^{q^{\mathcal{E}}}.\end{aligned}$$

For an arbitrary finite place w of $K(N)$, the ultrametric triangle inequality gives

$$|x|_w \leq \max(|\tilde{\varphi}|_{K(N)}(\alpha)|_w, |\alpha^{q^{\mathcal{E}}}|_w) \leq \max(1, |\tilde{\varphi}|_{K(N)}(\alpha)|_w)\max(1, |\alpha|_w)^{q^{\mathcal{E}}}.$$

For the infinite places w we have to take a little detour. We define

$$\beta = \frac{\tilde{\varphi}|_{K(N)}(\alpha)}{\alpha^{q^{\mathcal{E}}}} \in \overline{\mathbb{Q}} \setminus \{1\}$$

and bound

$$\begin{aligned}|x|_w &= |\beta-1|_w|\alpha^{q^{\mathcal{E}}}|_w \leq |\beta-1|_w \max(1,|\alpha^{q^{\mathcal{E}}}|_w)\\ &\leq |\beta-1|_w \max(1,|\tilde{\varphi}|_{K(N)}(\alpha)|_w)\max(1,|\alpha^{q^{\mathcal{E}}}|_w)\end{aligned}$$

instead. We get

$$\begin{aligned}0 &= \sum_w d_w \log|x|_w\\ &= \sum_{w|p} d_w \log|x|_w + \sum_{w\nmid p, w|\infty} d_w \log|x|_w + \sum_{w|\infty} d_w \log|x|_w\\ &\leq \sum_{w|p} d_w \log(p^{-\frac{1}{\mathcal{E}}}\max(1,|\tilde{\varphi}|_{K(N)}(\alpha)|_w)\max(1,|\alpha^{q^{\mathcal{E}}}|_w))\\ &\quad + \sum_{w\nmid p, w|\infty} d_w \log(\max(1,|\tilde{\varphi}|_{K(N)}(\alpha)|_w)\max(1,|\alpha^{q^{\mathcal{E}}}|_w))\\ &\quad + \sum_{w|\infty} d_w \log(|\beta-1|_w\max(1,|\tilde{\varphi}|_{K(N)}(\alpha)|_w)\max(1,|\alpha^{q^{\mathcal{E}}}|_w)).\end{aligned}$$

After dividing by $[K(N):\mathbb{Q}]$ this gives

$$\frac{\log p}{\mathcal{E}} - \frac{1}{[K(N):\mathbb{Q}]}\sum_{w|\infty} d_w \log|\beta-1|_w \leq (1+q^{\mathcal{E}})h(\alpha). \tag{5.12}$$

Let us now assume that $h(\beta)\leq\frac{1}{4}, [\mathbb{Q}(\beta):\mathbb{Q}]\geq 16$ and $h(\alpha)\leq 1$. This is without loss of generality since otherwise the conclusion of the Lemma is clear. By Lemma 4.19 with $\delta=\frac{1}{4}$ we get

$$\begin{aligned}\frac{1}{[K(N):\mathbb{Q}]}\sum_{\tau:\mathbb{Q}(\beta)\to\mathbb{C}}\log|\tau(\beta)-1| &= \frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]}\sum_{\tau:\mathbb{Q}(\beta)\to\mathbb{C}}\log|\tau(\beta)-1|\\ &\leq 5\cdot 2^{11}h(\beta)^{\frac{1}{4}}\\ &\leq 5\cdot 2^{11}((1+q^{\mathcal{E}})h(\alpha))^{\frac{1}{4}}.\end{aligned}$$

Together with estimate (5.12) we get

$$\frac{\log p}{\mathcal{E}} - 5\cdot 2^{11}((1+q^{\mathcal{E}})h(\alpha))^{\frac{1}{4}} \leq (1+q^{\mathcal{E}})h(\alpha).$$

Hence

$$\frac{\log p}{\mathcal{E}} \leq (1+q^{\mathcal{E}})(1+5\cdot 2^{11})h(\alpha)^{\frac{1}{4}}$$

which gives

$$\left(\frac{\log p}{\mathcal{E}(1+q^{\mathcal{E}})(1+5\cdot 2^{11})}\right)^4 \leq h(\alpha).$$

□

5.3 The wildly ramified case

Again, we fix E, F, K, p and $p^2 = q$ as in section 5.1. For this whole section we will only consider the case where $p^2|N$. Let v be the place of F above p. Recall that we considered F as a subfield of $\overline{\mathbb{Q}_p}$, hence for an element $\alpha \in F$ we can consider $|\alpha|_p$.

Lemma 5.18
Let $\psi \in \mathrm{Gal}(\mathbb{Q}_q(N)/\mathbb{Q}_q(N/p))$. Then $\psi|_{F\cap\mathbb{Q}_q(N)} = \mathrm{id}$.

Proof
By Lemma 5.5 we have $\mathbb{Q}_q(N)\cap F = \mathbb{Q}_q(N/p)\cap F$. Since $\psi \in \mathrm{Gal}(\mathbb{Q}_q(N)/\mathbb{Q}_q(N/p))$, ψ must be the identity on $\mathbb{Q}_q(N/p)$, hence also on $\mathbb{Q}_q(N/p) \cap F = \mathbb{Q}_q(N) \cap F$. □

Lemma 5.19
Let $\alpha \in F(N)$. Then

$$|\psi(\alpha)^q - \alpha^q|_p \leq p^{-1} \max(1, |\psi(\alpha)|_p)^q \max(1, |\alpha|_p)^q \tag{5.13}$$

for all $\psi \in \mathrm{Gal}(F(N)/F(N/p))$.

Proof
First, we suppose $|\alpha|_p \leq 1$. Let $\psi \in \mathrm{Gal}(F(N)/F(N/p))$ and consider the restriction $\psi|_{F(p^n)} \in \mathrm{Gal}(F(p^n)/F(p^{n-1}))$. By Lemma 5.9 this is an element of $G_i(F(N)/F)$ for $i = q^{n-1} - 1$.

By the definition of the ramification group, this means

$$\psi(\alpha) - \alpha \in \mathfrak{P}^{q^{n-1}}$$

where $\mathfrak{P}$ is the maximal ideal in the ring of integers of $F(N)$. By Lemmas 5.7 and 5.8 (ii) the ramification index e of $F(N)/F$ is at most $q^{n-1}(q-1) \leq q^n$. Therefore, $(\psi(\alpha) - \alpha)^q \in \mathfrak{P}^{q^n} \subset \mathfrak{P}^e$. Since $p \in \mathfrak{P}^e$ we conclude

$$0 \equiv (\psi(\alpha) - \alpha)^q \equiv \psi(\alpha)^q - \alpha^q \bmod \mathfrak{P}^e.$$

This leads to $|\psi(\alpha^q) - \alpha^q|_p \leq |p|_p = p^{-1}$. Hence the statement follows if $|\alpha|_p \leq 1$. Now for $|\alpha|_p > 1$ consider α^{-1} with $|\alpha^{-1}|_p \leq 1$. We get $|\psi(\alpha)^{-q} - \alpha^{-q}|_p \leq p^{-1}$ and

$$|\alpha^{-q}(\psi(\alpha)^q - \alpha^q)|_p = |(\alpha^{-q} - \psi(\alpha)^{-q})\psi(\alpha)^q|_p \leq p^{-1}|\psi(\alpha)^q|_p.$$

After multiplying by $|\alpha^q|_p$ we obtain our statement. □

Lemma 5.20
Let $\psi \in \mathrm{Gal}(K(N)/K(N/p))$ and v be the place of $K(N)$ above p. Let

$$G = \{\sigma \in \mathrm{Gal}(K(N)/\mathbb{Q}) | \sigma\psi\sigma^{-1} = \psi\}$$

be the centralizer of ψ. Then

$$|Gv| \geq \frac{[K(N) : \mathbb{Q}]}{p^4 d_v}.$$

Proof
Let $H := \mathrm{Gal}(K(N)/K(N/p))$, it is a normal subgroup of $\mathrm{Gal}(K(N)/\mathbb{Q})$. The orbit of ψ under conjugation by $\mathrm{Gal}(K(N)/\mathbb{Q})$ is contained in H. The stabilizer of this action is G so we can use the orbit-stabilizer theorem. Furthermore, by the proof of Lemma 5.2 of [Hab13], we have $|\mathrm{Gal}(\mathbb{Q}(N)/\mathbb{Q}(N/p))| \leq p^4$. Since H is isomorphic to a subgroup of that group, we have $|H| \leq p^4$. We get

$$|G| \geq \frac{|\mathrm{Gal}(K(N)/\mathbb{Q})|}{|H|} = \frac{[K(N):\mathbb{Q}]}{|H|} \geq \frac{[K(N):\mathbb{Q}]}{p^4}.$$

Furthermore, again by the orbit-stabilizer theorem, for a place v of $K(N)$ above p we have

$$|Gv| = \frac{|G|}{|\mathrm{Stab}_G(v)|} \geq \frac{[K(N):\mathbb{Q}]}{p^4|\mathrm{Stab}_G(v)|}. \tag{5.14}$$

The Galois group $\mathrm{Gal}(K(N)/\mathbb{Q})$ acts transitively on all places of $K(N)$ lying above p and the total number of such places is $\frac{[K(N):\mathbb{Q}]}{d_v}$ since $K(N)$ is a Galois extension of $\mathbb{Q}$. The number of places is by the orbit-stabilizer theorem again the same as

$$\frac{|\mathrm{Gal}(K(N)/\mathbb{Q})|}{|\mathrm{Stab}_{\mathrm{Gal}(K(N)/\mathbb{Q})}(v)|}$$

.

This gives us the following inequality:

$$|\mathrm{Stab}_G(v)| \leq |\mathrm{Stab}_{\mathrm{Gal}(K(N)/\mathbb{Q})}(v)| = d_v.$$

After inserting this in equation 5.14 we get

$$|Gv| \geq \frac{[K(N):\mathbb{Q}]}{p^4|\mathrm{Stab}_G(v)|} \geq \frac{[K(N):\mathbb{Q}]}{p^4 d_v}. \tag{5.15}$$

□

The next height bound is the analogue of Lemma 5.3 of [Hab13].

Lemma 5.21
Let $\alpha \in K(N)\backslash\mu_\infty$ be non-zero and let $n \geq 2$ be the greatest integer with $p^n \mid N$. If $\alpha^q \notin F(N/p)$, then

$$h(\alpha) \geq \frac{(\log p)^4}{4 \cdot 10^6 p^{32}}. \tag{5.16}$$

Proof
By hypothesis we may chose $\psi \in \mathrm{Gal}(F(N)/F(N/p))$ with $\psi(\alpha^q) \neq \alpha^q$.

We let

$$x = \psi(\alpha^q) - \alpha^q$$

and observe $x \neq 0$ by our choice of ψ. So

$$\sum_v d_v \log |x|_v = 0 \tag{5.17}$$

by the product formula.

Say $G = \{\sigma \in \mathrm{Gal}(K(N)/\mathbb{Q}) | \sigma\psi\sigma^{-1} = \psi\}$ as in Lemma 5.20 and v is the place of $K(N)$ coming from the restriction of the p-adic valuation on $\overline{\mathbb{Q}_p}$ to $K(N)$. Let $\sigma \in G$. The place σv of $K(N)$ satisfies $|\sigma(y)|_{\sigma v} = |y|_v$ for all $y \in K(N)$. So

$$|(\sigma\psi\sigma^{-1})(\alpha^q) - \alpha^q|_{\sigma v} = |\psi(\sigma^{-1}(\alpha^q)) - \sigma^{-1}(\alpha^q)|_p.$$

We may apply Lemma 5.19 to $\sigma^{-1}(\alpha)$. This implies

$$\begin{aligned} |(\sigma\psi\sigma^{-1})(\alpha^q) - \alpha^q|_{\sigma v} &= |\psi(\sigma^{-1}(\alpha))^q - \sigma^{-1}(\alpha)^q|_v \\ &\leq p^{-1} \max\{1, |\psi(\sigma^{-1}(\alpha))|_v\}^q \max\{1, |\sigma^{-1}(\alpha)|_v\}^q \\ &\leq p^{-1} \max\{1, |(\sigma\psi\sigma^{-1})(\alpha)|_{\sigma v}\}^q \max\{1, |\alpha|_{\sigma v}\}^q. \end{aligned}$$

Now $\sigma\psi\sigma^{-1} = \psi$ since $\sigma \in G$. Therefore,

$$|x|_w \leq p^{-1} \max\{1, |\psi(\alpha)|_w\}^q \max\{1, |\alpha|_w\}^q \text{ for all } w \in Gv. \tag{5.18}$$

If w is an arbitrary finite place of $K(N)$, the ultrametric triangle inequality implies

$$|x|_w \leq \max\{1, |\psi(\alpha)|_w\}^q \max\{1, |\alpha|_w\}^q. \tag{5.19}$$

Now let w be an infinite place. We define

$$\beta = \frac{\psi(\alpha^q)}{\alpha^q} \in \overline{\mathbb{Q}} \backslash \{1\}$$

and bound the following expression instead:

$$|x|_w = |\beta - 1|_w |\alpha^q|_w \leq |\beta - 1|_w \max\{1, |\alpha|_w\}^q. \tag{5.20}$$

We split the sum (5.17) up into the finite places in Gv, the remaining finite places, and the infinite places and the continue like in the proof of Lemma5.17. The esti-

mates 5.18, (5.19) and (5.20) together with the product formula (5.17) imply

$$\begin{aligned}
0 &\leq \sum_{w\in Gv} d_w(\log p^{-1} + q\log(\max\{1,|\psi(\alpha)|_w\}\max\{1,|\alpha|_w\})) \\
&\quad + \sum_{w\nmid\infty, w\notin Gv} d_w q\log(\max\{1,|\psi(\alpha)|_w\}\max\{1,|\alpha|_w\}) \\
&\quad + \sum_{w|\infty} d_w(\log|\beta-1|_w + q\log\max\{1,|\alpha|_w\}) \\
&= \sum_{w\in Gv} d_w \log p^{-1} \\
&\quad + \sum_{w\nmid\infty} d_w q\log(\max\{1,|\psi(\alpha)|_w\}\max\{1,|\alpha|_w\}) \\
&\quad + \sum_{w|\infty} d_w(\log|\beta-1|_w + q\log\max\{1,|\alpha|_w\}) \\
&\leq \sum_{w\in Gv} d_w \log p^{-1} \\
&\quad + \sum_{w} d_w q\log(\max\{1,|\psi(\alpha)|_w\}\max\{1,|\alpha|_w\}) \\
&\quad + \sum_{w|\infty} d_w \log|\beta-1|_w. \qquad (5.21)
\end{aligned}$$

Moreover, since the action of the Galois group is transitive and all fields here are Galois over $\mathbb{Q}$, all local degrees d_w with $w \in Gv$ equal d_v. So

$$\sum_{w\in Gv} d_w \log p^{-1} = d_v \log p^{-1}|Gv| \leq -d_v \log p \frac{[K(N):\mathbb{Q}]}{p^4 d_v}$$

by Lemma 5.20. We use this estimate together with (5.21) and after dividing by $[K(N):\mathbb{Q}]$ we obtain

$$0 \leq -\frac{\log p}{p^4} + \frac{1}{[K(N):\mathbb{Q}]}\left(\sum_{w|\infty} d_w \log|\beta-1|_w\right) + qh(\psi(\alpha)) + qh(\alpha).$$

Also, $h(\psi(\alpha)) = h(\alpha)$ and $q = p^2$, hence

$$\frac{\log p}{p^4} \leq \frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]}\left(\sum_{\tau:\mathbb{Q}(\beta)\hookrightarrow\mathbb{C}} \log|\tau(\beta)-1|\right) + 2p^2 h(\alpha).$$

By construction we certainly have $\beta \neq 0, 1$ and in order to apply Lemma 4.19 it remains to show that β is not a root of unity. If we assume the contrary, then $\frac{\psi(\alpha)}{\alpha}$ will be a root of unity too. Lemma 5.12 implies $\left(\frac{\psi(\alpha)}{\alpha}\right)^q = 1$ which contradicts our assumption on α.

We have $h(\beta) \leq h(\psi(\alpha^q)) + h(\alpha^q) \leq 2p^2 h(\alpha)$. Assuming $h(\beta) \leq \frac{1}{4}$ (which we can do since otherwise we would have a lower bound for $h(\alpha)$ that is better than the claim), we apply Lemma 4.19 with $\delta = \frac{1}{4}$ and get:

$$\begin{aligned}\frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]} \sum_{\tau:\mathbb{Q}(\beta)\hookrightarrow\mathbb{C}} \log|\tau(\beta)-1| &\leq 5 \cdot 2^{11} h(\beta)^{\frac{1}{4}} \\ &\leq 5 \cdot 2^{11} (2p^2 h(\alpha))^{\frac{1}{4}}\end{aligned}$$

and hence

$$\begin{aligned}\frac{\log p}{p^4} &\leq 5 \cdot 2^{11} (2p^2 h(\alpha))^{\frac{1}{4}} + 2p^2 h(\alpha) \\ &\leq 5 \cdot 2^{11} (2p^2 h(\alpha))^{\frac{1}{4}} + 2p^2 h(\alpha)^{\frac{1}{4}} \\ &\leq (5 \cdot 2^{11} (2p^2)^{\frac{1}{4}} + 2p^2) h(\alpha)^{\frac{1}{4}}.\end{aligned}$$

We solve the above inequality for $h(\alpha)$:

$$\begin{aligned}h(\alpha) &> \left(\frac{\log p}{(5 \cdot 2^{11} (2p^2)^{\frac{1}{4}} + 2p^2) p^4}\right)^4 \\ &\geq \left(\frac{\log p}{(5 \cdot 2^{11} 2^{\frac{1}{4}} p^{\frac{1}{2}} + 2p^4) p^4}\right)^4 \\ &\geq \left(\frac{\log p}{(6093 p^{-\frac{7}{2}} + 1) 2p^8}\right)^4 \\ &\geq \left(\frac{\log p}{44 p^8}\right)^4 \\ &= \frac{(\log p)^4}{4 \cdot 10^6 p^{32}}.\end{aligned}$$

□

5.4 Descent and the final bound

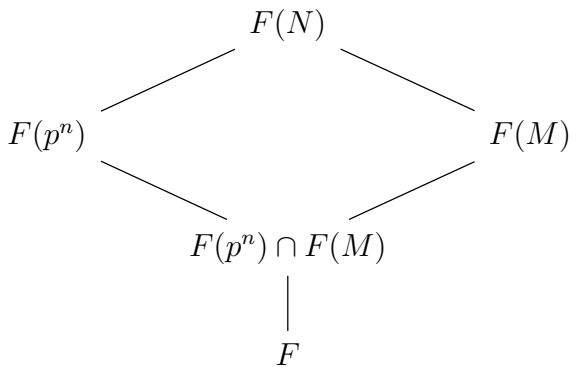
Again, we fix E, L and p as in section 5.1. Let also $\mathcal{E}$ be a multiple of $[F:\mathbb{Q}_p](q-1)$. Now we want to turn the conditional bound in the ramified case in an unconditional bound using some descent method. First, we construct a useful automorphism of $K(N)/\mathbb{Q}$.

Lemma 5.22
Let $n \geq 0$ be the greatest integer with $p^n \mid N$. There exists $\sigma_F \in \mathrm{Gal}(F(N)/F)$, lying in the center of $\mathrm{Gal}(K(N)/K)$ such that $\sigma_F(\zeta) = \zeta^{4^{[F:\mathbb{Q}_q]}}$ for all $\zeta \in \mu_{p^n}$. Moreover, σ_F acts on $E[p^n]$ as multiplication by $2^{[F:\mathbb{Q}_q]}$.

Proof
Before we prove this Lemma, let us recall that by Lemma 5.10 $F(N)$ contains μ_{p^n}.

Since p is odd, Lemma 5.8 (v) implies that there is $\sigma'_F \in \mathrm{Gal}(F(p^n)/F)$ that acts on $E[p^n]$ as multiplication by $2^{[F:\mathbb{Q}_q]}$. Since the Weil pairing $\langle \cdot, \cdot \rangle$ is surjective, we can find for every root of unity $\zeta \in \mu_{p^n}$ points $P, Q \in E[p^n]$ such that $\langle P, Q \rangle = \zeta$. Now $\sigma'_F(\langle P, Q \rangle) = \langle \sigma'_F(P), \sigma'_F(Q) \rangle = \langle 2^{[F:\mathbb{Q}_q]}P, 2^{[F:\mathbb{Q}_q]}Q \rangle = \langle P, Q \rangle^{4^{[F:\mathbb{Q}_q]}}$. Hence σ'_F acts on μ_{p^n} as raising to the $4^{[F:\mathbb{Q}_q]}$-th power.

We will now lift the automorphism σ'^{q-1}_F to $\sigma^{q-1}_F \in \mathrm{Gal}(F(N)/F(M))$. For that we consider the following diagram



and we will prove that $\sigma'^{q-1}_F|_{F(p^n)\cap F(M)}$ is the identity.

We know that $F(M)/F$ is unramified by Lemma 5.8 (ii), hence its subextension $F(p^n) \cap F(M)/F$ is also unramified. But on the other hand, $F(p^n)/F(p)$ is totally ramified by Lemma 5.7, hence $F(p^n) \cap F(M)$ has to be a subfield of $F(p)$ which has degree $q-1$ over F. Hence we get that $[F(p^n) \cap F(M) : F]$ divides $q-1$.

So σ'^{q-1}_F is already in $\mathrm{Gal}(F(p^n)/F(p^n) \cap F(M))$ which is by the above diagram isomorphic to $\mathrm{Gal}(F(N)/F(M))$. We will call the image of σ'^{q-1}_F under this isomorphism σ^{q-1}_F.

Taking the sum of points gives an isomorphism between $E[p^n] \times E[M]$ and $E[N]$ which is compatible with the action of $\mathrm{Gal}(K(N)/K)$. Since σ_F acts as multiplication by $2^{[F:\mathbb{Q}_q]}$ on $E[p^n]$ and trivially on $E[M]$ and F (hence also on K), it must lie in the center of $\mathrm{Gal}(K(N)/K)$. □

5.4.1 Some group theory

Lemma 5.23
For $p \neq 2$ the vector space $V := \{A \in \mathrm{Mat}_2(\mathbb{F}_p) | \operatorname{Tr} A = 0\}$ has only trivial subvector spaces that are invariant under conjugation with $\mathrm{SL}_2(\mathbb{F}_p)$.

Proof
Let U be a non-trivial subvector space of V that is invariant under conjugation by $\mathrm{SL}_2(\mathbb{F}_p)$. By considering the non-degenerate scalar product $\langle A, B \rangle := \operatorname{Tr}(A^T B)$ on

V we can show that $U^\perp$ is also invariant: Let $A \in U^\perp$ and $B \in U$. Then for any $S \in \mathrm{SL}_2(\mathbb{F}_p)$ we have $\mathrm{Tr}((SAS^{-1})^T B) = \mathrm{Tr}(S^{-T}(A^T S^T B)) = \mathrm{Tr}((A^T S^T B)S^{-T}) = \mathrm{Tr}(A^T(S^T B S^{-T})) = \mathrm{Tr}(A^T B')$ for some $B' \in U$ since U is invariant under conjugation. But then $\mathrm{Tr}(A^T B') = 0$, hence $SAS^{-1} \in U^\perp$. We know that V has dimension three. Now if U is an invariant subvector space of dimension 2, its orthogonal complement has to be of dimension one and we get that V has only trivial invariant subvector spaces if and only if it does not have a one-dimensional invariant subvector space which is what we will prove now.

Let $U \subset V$ be invariant under conjugation by $\mathrm{SL}_2(\mathbb{F}_p)$ and of dimension one. Then there must be a matrix $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ non-zero, such that $U = \{0, A, 2A, \ldots, (p-1)A\}$. Consider $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and

$$S \begin{pmatrix} a & b \\ c & -a \end{pmatrix} S^{-1} = \begin{pmatrix} a+c & -2a-c+b \\ c & -a-c \end{pmatrix} \stackrel{!}{=} \lambda \begin{pmatrix} a & b \\ c & -a \end{pmatrix}.$$

So in order for U to be invariant, we have to have $c = 0$ and $\lambda = 1$, which also gives $a = 0$. Hence U must be the matrices. Let us assume that space of matrices is invariant. Then the orthogonal complement is $U^\perp = \{\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{F}_p)\}$. But here we can again find that conjugation by S does not stay within $U^\perp$. Let $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in U^\perp$. Then

$$SAS^{-1} = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \notin U^\perp.$$

We excluded all possibilities of one-dimensional invariant subvector spaces and proved the lemma. □

Lemma 5.24
Let $p \geq \exp(\mathrm{Gal}(K/\mathbb{Q}))$. *Then* $\rho(\mathrm{Gal}(K(p)/K))$ *contains* $\mathrm{SL}_2(\mathbb{F}_p)$.

Proof
By property (P2), we have $\rho(\mathrm{Gal}(K(p)/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{F}_p)$. Consider the normal subgroup $N := \mathrm{Gal}(K(p)/K)$ of $\mathrm{Gal}(K(p)/\mathbb{Q})$. Then $\mathrm{Gal}(K(p)/\mathbb{Q})/N$, which is isomorphic to $\mathrm{Gal}(K/\mathbb{Q})$, has exponent $\exp(\mathrm{Gal}(K/\mathbb{Q}))$. So also $\rho(\mathrm{Gal}(K(p)/\mathbb{Q}))/\rho(N)$ has exponent dividing $\exp(\mathrm{Gal}(K/\mathbb{Q}))$. Consider

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p) \Rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \rho(\mathrm{Gal}(K(p)/\mathbb{Q})).$$

Take the $\exp(\mathrm{Gal}(K/\mathbb{Q}))$-th power of this matrix and get an element of $\rho(N)$ (recall that $\exp(\mathrm{Gal}(K/\mathbb{Q}))$ is coprime to p):

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\exp(\mathrm{Gal}(K/\mathbb{Q}))} = \begin{pmatrix} 1 & \exp(\mathrm{Gal}(K/\mathbb{Q})) \\ 0 & 1 \end{pmatrix} \in \rho(N) \cap \mathrm{SL}_2(\mathbb{F}_p).$$

Since $\rho(N)$ is normal in $\rho(\mathrm{Gal}(K(p)/\mathbb{Q}))$, then also $\rho(N) \cap \mathrm{SL}_2(\mathbb{F}_p)$ is normal in $\mathrm{SL}_2(\mathbb{F}_p)$. By Theorem 8.4 of [Lan02], hence the only normal subgroups of $\mathrm{SL}_2(\mathbb{F}_p)$ are $\{1\}, \{\pm 1\}, \mathrm{SL}_2(\mathbb{F}_p)$. But since we found one element in $\rho(N) \cap \mathrm{SL}_2(\mathbb{F}_p)$ that is not in $\{\pm 1\}$, we get $\rho(N) \cap \mathrm{SL}_2(\mathbb{F}_p) = \mathrm{SL}_2(\mathbb{F}_p)$. □

Lemma 5.25
Let $p \geq 3$ and let G be a subgroup of $\mathrm{Mat}_2(\mathbb{F}_p)$ of order p^2 that contains at least one non-zero scalar matrix. Let V be the subgroup of $\mathrm{Mat}_2(\mathbb{F}_p)$ generated by ABA^{-1} where B varies over G and A varies over $\mathrm{SL}_2(\mathbb{F}_p)$. Then $V = \mathrm{Mat}_2(\mathbb{F}_p)$.

Proof
Since G has more than p elements, there must be a non-scalar matrix in G. So let $B \in G$ be a non-scalar matrix. Then since scalar matrices are the only matrices that commute with all elements on $\mathrm{SL}_2(\mathbb{F}_p)$, there must be $A \in \mathrm{SL}_2(\mathbb{F}_p)$ such that $ABA^{-1} \neq B$. Then $\mathrm{Tr}(ABA^{-1} - B) = \mathrm{Tr}(ABA^{-1}) - \mathrm{Tr}(B) = \mathrm{Tr}(B) - \mathrm{Tr}(B) = 0$ and $V^0 := \{B \in V | \, \mathrm{Tr}(B) = 0\} \neq \{0\}$. Since the action by conjugation of $\mathrm{SL}_2(\mathbb{F}_p)$ on $\{B \in \mathrm{Mat}_2(\mathbb{F}_p) | \, \mathrm{Tr}(B) = 0\}$ leaves only the trivial subvector spaces invariant and V^0 is not just the zero vector, we find that $V^0 = \{B \in \mathrm{Mat}_2(\mathbb{F}_p) | \, \mathrm{Tr}(B) = 0\}$ which has dimension 3. Now since for $p > 2$ the identity matrix is an element of V, but not of V^0, we have $V \supsetneq V^0$. But since V^0 is an $\mathbb{F}_p$-vector space of dimension 3 (hence has order p^3) and V is strictly larger than V^0 (hence has to have order strictly larger than p^3), we get $V = \mathrm{Mat}_2(\mathbb{F}_p)$. □

5.4.2 The actual descent

Lemma 5.26
Let $G := \mathrm{Gal}(F(N)/F(N/p))$. Suppose E and p satisfy (P1) and (P2). We assume $p^2 \mid N$. Then:

(i) The subgroup of $H := \mathrm{Gal}(K(N)/K)$ generated by the conjugates of G equals $\mathrm{Gal}(K(N)/K(N/p))$.

(ii) If $\alpha \in K(N)$ with $\sigma(\alpha) \in F(N/p)$ for all $\sigma \in \mathrm{Gal}(K(N)/K)$, then $\alpha \in K(N/p)$.

Proof
(i) We will follow closely the proof of Habegger's Lemma 6.2 but we will not use the concept of non-split Cartan subgroups as in Habegger's proof. Instead we will use the lemmas above to show that the group in (i) is big enough.

We have

$$H \subset \mathrm{Gal}(K(N)/K(N/p)) \tag{5.22}$$

and we will show the equality.

We now want to look at the Galois representations and choose a basis for each $E[N]$ that is compatible with the diagram below.

$$\tilde{\rho} : \mathrm{Gal}(K(p)/K) \to \mathrm{GL}_2(\mathbb{F}_p) \text{ and } \rho : \mathrm{Gal}(K(N)/K) \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

and put them into the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(K(N)/K) & \xrightarrow{\rho} & \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K(N/p)/K) & \xrightarrow{\rho|_{K(N/p)}} & \mathrm{GL}_2(\mathbb{Z}/p^{n-1}\mathbb{Z}) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K(p)/K) & \xrightarrow{\tilde{\rho}} & \mathrm{GL}_2(\mathbb{F}_p) \end{array} \tag{5.23}$$

The right vertical arrows are the natural surjections and the left vertical arrows are induced by the restrictions. By Lemma 5.24 we know that $\tilde{\rho}(\mathrm{Gal}(K(p)/K))$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. We will now construct a homomorphism $\mathcal{L}$ from $\mathrm{Gal}(K(N)/K(N/p))$ to $\mathrm{Mat}_2(\mathbb{F}_p)$ which will firstly show by its injectivity that $|H| \leq p^4$ and secondly, through Lemma 5.25, show equality.

If $\sigma \in \mathrm{Gal}(K(N)/K(N/p))$ then $\rho(\sigma)$ is represented by $1+p^{n-1}\mathcal{L}'(\sigma)$ with $\mathcal{L}'(\sigma) \in \mathrm{Mat}_2(\mathbb{Z})$. Moreover, $\mathcal{L}'(\sigma)$ is well-defined modulo $p\,\mathrm{Mat}_2(\mathbb{Z})$. We obtain by reduction mod p a "logarithm" $\mathcal{L} : \mathrm{Gal}(K(N)/K(N/p)) \to \mathrm{Mat}_2(\mathbb{F}_p)$. The name comes from the following property: Let $\sigma_1, \sigma_2 \in \mathrm{Gal}(K(N)/K(N/p))$, then

$$\rho(\sigma_1\sigma_2) = (1+p^{n-1}\mathcal{L}(\sigma_1))(1+p^{n-1}\mathcal{L}(\sigma_2)) \equiv 1+p^{n-1}(\mathcal{L}(\sigma_1)+\mathcal{L}(\sigma_2)) \bmod p^n\,\mathrm{Mat}_2(\mathbb{Z})$$

where we let $\mathcal{L}$ be the reduction of $\mathcal{L}'$ modulo $p\,\mathrm{Mat}_2(\mathbb{Z})$. So $\mathcal{L}(\sigma_1\sigma_2) = \mathcal{L}(\sigma_1) + \mathcal{L}(\sigma_2)$, hence $\mathcal{L}$ is a group homomorphism. We want to show that $\mathcal{L}$ is injective. Let $\sigma \in \mathrm{Gal}(K(N)/K(N/p))$ be such that $\mathcal{L}(\sigma) = \mathrm{id}$ in $\mathrm{Mat}_2\,\mathbb{F}_p$. This means that $\rho(\sigma) = 1$ in $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$. We look at the diagram (**??**) and see that this means that σ fixes $K(p^n)$. Since it is an element of $\mathrm{Gal}(K(N)/K(N/p)$, it also fixes $K(N/p)$, hence fixes $K(N)$. So $\sigma \in \mathrm{Gal}(K(N)/K(N/p))$ is the identity and $\mathcal{L}$ is injective.

Hence we get

$$[K(N) : K(N/p)] \leq |\,\mathrm{Mat}_2(\mathbb{F}_p)| = p^4. \tag{5.24}$$

If $\sigma \in \mathrm{Gal}(K(N)/K)$ and $\psi \in G$ then $\sigma\psi\sigma^{-1} \in \mathrm{Gal}(K(N)/K(N/p))$ and we get

$$\rho(\sigma\psi\sigma^{-1}) \equiv 1 + p^{n-1}\tilde{\rho}(\sigma)\mathcal{L}'(\psi)\tilde{\rho}(\sigma)^{-1} \bmod p^n\,\mathrm{Mat}_2(\mathbb{Z}).$$

Hence

$$\mathcal{L}(\sigma\psi\sigma^{-1}) = \tilde{\rho}(\sigma)\mathcal{L}(\psi)\tilde{\rho}(\sigma)^{-1}. \tag{5.25}$$

By Lemma 5.8 (iv), G has order p^2, so $|\mathcal{L}(G)| = p^2$ by injectivity of $\mathcal{L}$.

We recall that by Lemma 5.24 the image of $\tilde{\rho}$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. So the definition of H and equation (5.25) imply that conjugating a matrix in $\mathcal{L}(G)$ by an element of $\mathrm{SL}_2(\mathbb{F}_p)$ stays within $\mathcal{L}(H)$. We want to apply Lemma 5.25 to $\mathcal{L}(G)$ to deduce $\mathcal{L}(H) = \mathrm{Mat}_2(\mathbb{F}_p)$. Then $|\mathcal{L}(H)| = |H| = p^4$ and by (5.24), H has to be equal to $\mathrm{Gal}(K(N)/K(N/p))$. For applying Lemma 5.25 we have to prove that $\mathcal{L}(G)$ contains a non-zero scalar matrix:

By Lemma 5.8 (v) we know that the image of the Galois representation $\mathrm{Gal}(F(p^n)/F) \to \mathrm{Aut}\, E[p^n]$ contains multiplication by $M^{[F:\mathbb{Q}_q]}$ for any M coprime to p. We now want to construct an element in $\mathrm{Gal}(F(p^n)/F(p^{n-1}))$ whose image is scalar multiplication. Let M be a generator of $(\mathbb{Z}/p^n\mathbb{Z})^*$, then the multiplication by M will have order $(p-1)p^{n-1}$ in $\mathrm{Aut}\, E[p^n]$.

Now by Lemma 5.22 we know that there exists $\sigma'_F \in \mathrm{Gal}(F(p^n)/F)$ such that its image is the multiplication by $M^{[F:\mathbb{Q}_q]}$. We want to show that $\sigma_F'^{(q-1)p^{n-2}}$ is an element of $\mathrm{Gal}(F(p^n)/F(p^{n-1}))$ and that it is not trivial. We start with the non-triviality. Consider $\mathrm{Gal}(F(p^n)/F)/\mathrm{Gal}(F(p^n)/F(p^{n-1}) \cong \mathrm{Gal}(F(p^{n-1})/F)$. Since $\mathrm{Gal}(F(p^n)/F)$ is isomorphic to $A \times (\mathbb{Z}/p^{n-1}\mathbb{Z})^2$ where A is a subgroup of $\mathbb{Z}/(q-1)\mathbb{Z}$ (see the proof of Lemma 5.10), its exponent will be ap^{n-1} where $a \mid (q-1)$. But $[F:\mathbb{Q}_q]$ is not a multiple of ap^{n-1} since $[F:\mathbb{Q}_q]$ is coprime to p. Hence $\sigma_F'^{(q-1)p^{n-2}}$ is not trivial.

Now consider $\mathrm{Gal}(F(p^{n-1})/F)$. This is isomorphic to $A \times (\mathbb{Z}/p^{n-2}\mathbb{Z})^2$ where A is a subgroup of $\mathbb{Z}/(q-1)\mathbb{Z}$ and its exponent will be ap^{n-2} where $a \mid (q-1)$. On the other hand, $[F:\mathbb{Q}_q](q-1)p^{n-2}$ is now a multiple of $(q-1)p^{n-2}$, hence the restriction of $\sigma_F'^{(q-1)p^{n-2}}$ to $F(p^{n-1}))$ is trivial which means that it has to be in $\mathrm{Gal}(F(p^n)/F(p^{n-1}))$.

By Lemma 5.8 (iv), we have $\mathrm{Gal}(F(p^n)/F(p^{n-1})) \cong \mathrm{Gal}(F(N)/F(N/p))$, hence we can find $\sigma_F \in \mathrm{Gal}(F(N)/F(N/p))$ that gets mapped to σ'_F under that isomorphism. We can apply $\mathcal{L}$ to find that $\mathcal{L}(\mathrm{Gal}(F(N)/F(N/p)))$ contains an element that acts as scalar multiplication on the p^n-torsion points, hence has to be a scalar matrix.

(ii) Now we proceed with the second part. Let $\alpha \in K(N)$ with $\sigma(\alpha) \in F(N/p)$ for all $\sigma \in \mathrm{Gal}(K(N)/K)$. Since we can invert elements of Galois groups, it makes sense to consider σ^{-1} whenever $\sigma \in \mathrm{Gal}(K(N)/K)$ and with the first part of the Lemma we get that the group generated by $\sigma\psi\sigma^{-1}$ equals $\mathrm{Gal}(K(N)/K(N/p))$. Since α is fixed by such a $\sigma\psi\sigma^{-1}$, it has to be in $K(N/p)$ which is what we wanted to show. $\square$

The technique of the descent used in the following theorem has been developed by Amoroso and Zannier in Section 4 of [AZ10].

Theorem 5.27
Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Let L be a Galois extension of $\mathbb{Q}$. Suppose there exists $d \in \mathbb{N}$ such that L has uniformly bounded local degrees above all but finitely many primes where d is the said uniform bound. Then there is a prime number p satisfying (5.1), (5.2), (5.3) and (5.4). If $\alpha \in L(E_{tor})^* \backslash \mu_\infty$, then

$$h(\alpha) \geq \frac{(\log p)^4}{p^{4p^4}}. \tag{5.26}$$

Proof
Again, we follow here the analogous proof of Proposition 6.1 of [Hab13] closely. Since E does not have complex multiplication, its j-invariant is neither 0, nor 1728. So the reduction of E at p is an elliptic curve with j-invariant neither 0, nor 1728 for all but finitely many primes p. By a Theorem of Serre [Ser72], all but finitely many of these p satisfy (P2). Furthermore, by [Elk87], there are infinitely many supersingular primes for an elliptic curve over $\mathbb{Q}$. We may thus fix a prime p satisfying (P1), (P2), (P3) and (P4) and set $q = p^2$.

Recall the following facts thet we fixed in the beginning of the chapter: Let $\alpha \in L(E_{\text{tor}})^* \backslash \mu_\infty$. Then $\alpha \in K(N)$ for some $N = p^n M$ with $M \in \mathbb{N}$ coprime to p, n a nonnegative integer and $K \subset L$ a number field that is Galois over $\mathbb{Q}$. Then we fix a finite Galois extension $F/\mathbb{Q}_q$ with $\mathbb{Q}_q \subset F \subset \overline{\mathbb{Q}_p}$ such that the v-adic completion of K is contained in F (where v extends p) and $[F : \mathbb{Q}_p]$ is uniformly bounded by d. Let furthermore $\mathcal{E} = (q-1)[F : \mathbb{Q}_q] \exp(\text{Gal}(L/\mathbb{Q}))$.

We take $\sigma_F \in \text{Gal}(F(N)/F)$ as in Lemma 5.22. If we are in the case of $p^2 \nmid N$, we can artificially choose an element in $\text{Gal}(F(p^2N)/F)$ and restrict it to $F(N)$. Then we define

$$\gamma = \frac{\sigma_F(\alpha)}{\alpha^{4^{[F:\mathbb{Q}_q]}}} \in K(N). \tag{5.27}$$

By the properties of the height we get

$$h(\gamma) \leq h(\sigma_F(\alpha)) + h(\alpha^{4^{[F:\mathbb{Q}_q]}}) = (4^{[F:\mathbb{Q}_q]} + 1)h(\alpha). \tag{5.28}$$

Let us start with the case of $n \geq 2$, hence $p^2 \mid N$. Since $\gamma \in K(N) \subset F(N)$, hence $\sigma(\gamma) \in K(N) \subset F(N)$ for all $\sigma \in \text{Gal}(K(N)/K)$, there is a least integer $n' \leq n$ such that $\sigma(\gamma) \in F(p^{n'}M)$ for all $\sigma \in \text{Gal}(K(N)/K)$. Lemma 5.26 implies that then also $\gamma \in K(p^{n'}M)$.

By minimality of n' there is a $\sigma \in \text{Gal}(K(N)/K)$ such that $\sigma(\gamma) \notin F(p^{n'-1}M)$. We will split this up into two cases: First $n' \geq 2$ and second $n' \leq 1$. We start with $n' \geq 2$. We apply σ to (5.27) and obtain

$$\sigma(\gamma) = \frac{\sigma(\sigma_F(\alpha))}{\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}}} = \frac{\sigma_F(\sigma(\alpha))}{\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}}} \tag{5.29}$$

since σ_F lies in the center of $\mathrm{Gal}(K(N)/K)$ by Lemma 5.22.

Next we want to apply Lemma 5.21 to $\sigma(\gamma)$, so we must verify that $\sigma(\gamma)^q \notin F(p^{n'-1}M)$. We will show this by contradiction, so assume $\sigma(\gamma)^q \in F(p^{n'-1}M)$.

Since $\sigma(\gamma) \notin F(p^{n'-1}M)$, there is $\psi \in \mathrm{Gal}(F(N)/F(p^{n'-1}M))$ such that $\psi(\sigma(\gamma)) \neq \sigma(\gamma)$. Furthermore, $\psi(\sigma(\gamma)^q) = \sigma(\gamma)^q$ by our assumption and so

$$\psi(\sigma(\gamma)) = \xi\sigma(\gamma) \text{ for some } \xi^q = 1 \text{ while } \xi \neq 1. \tag{5.30}$$

We apply ψ to equation (5.29) and obtain

$$\begin{aligned}\psi(\sigma(\gamma)) &= \frac{\psi(\sigma_F(\sigma(\alpha)))}{\psi(\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}})} \\ &= \frac{\sigma_F(\psi(\sigma(\alpha)))}{\psi(\sigma(\alpha))^{4^{[F:\mathbb{Q}_q]}}}\end{aligned}$$

since ψ commutes with σ_F (by Lemma 5.22). We define $\eta = \frac{\psi(\sigma(\alpha))}{\sigma(\alpha)} \neq 0$ and get, by (5.29) and (5.30)

$$\begin{aligned}\xi &= \frac{\psi(\sigma(\gamma))}{\sigma(\gamma)} \\ &= \frac{\psi\left(\frac{\sigma_F(\sigma(\alpha))}{\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}}}\right)}{\frac{\sigma_F(\sigma(\alpha))}{\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}}}} \\ &= \frac{\psi(\sigma_F(\sigma(\alpha)))\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}}}{\psi(\sigma(\alpha))^{4^{[F:\mathbb{Q}_q]}}\sigma_F(\sigma(\alpha))} \\ &= \frac{\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}}\psi(\sigma_F(\sigma(\alpha)))}{\psi(\sigma(\alpha))^{4^{[F:\mathbb{Q}_q]}}\sigma_F(\sigma(\alpha))} \\ &= \frac{\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}}}{\psi(\sigma(\alpha))^{4^{[F:\mathbb{Q}_q]}}}\frac{\psi(\sigma_F(\sigma(\alpha)))}{\sigma_F(\sigma(\alpha))} \\ &= \frac{\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}}}{\psi(\sigma(\alpha))^{4^{[F:\mathbb{Q}_q]}}}\frac{\sigma_F(\psi(\sigma(\alpha)))}{\sigma_F(\sigma(\alpha))} \\ &= \eta^{-4^{[F:\mathbb{Q}_q]}}\sigma_F(\eta) \\ &= \frac{\sigma_F(\eta)}{\eta^{4^{[F:\mathbb{Q}_q]}}}.\end{aligned}$$

Since ξ is a root of unity, we have $4^{[F:\mathbb{Q}_q]}h(\eta) = h(\eta^{4^{[F:\mathbb{Q}_q]}}) = h(\xi\eta^{4^{[F:\mathbb{Q}_q]}}) = h(\sigma_F(\eta)) = h(\eta)$, so $h(\eta) = 0$ and by Kronecker's Theorem, η is a root of unity.

We now fix $\widetilde{M} \in \mathbb{N}$ coprime to p such that $\eta^{\widetilde{M}} \in \mu_{p^\infty}$. Lemma 5.10 now implies that $\eta^{\widetilde{M}}$ is already in μ_{p^n} and by Lemma 5.22 we have $\sigma_F(\eta^{\widetilde{M}}) = (\eta^{\widetilde{M}})^{4^{[F:\mathbb{Q}_q]}}$. And we get

$$\sigma_F(\eta) = \xi'\eta^{4^{[F:\mathbb{Q}_q]}} \tag{5.31}$$

for some ξ' such that $\xi'^{\widetilde{M}} = 1$. Using equation (5.29) we get the following

$$\begin{aligned}\xi' &= \frac{\sigma_F(\eta)}{\eta^{4^{[F:\mathbb{Q}_q]}}} \\ &= \frac{\sigma_F(\psi(\sigma(\alpha)))}{\sigma_F(\sigma(\alpha))} \frac{\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}}}{\psi(\sigma(\alpha))^{4^{[F:\mathbb{Q}_q]}}} \\ &= \frac{\sigma_F(\psi(\sigma(\alpha)))}{\psi(\sigma(\alpha))^{4^{[F:\mathbb{Q}_q]}}} \frac{\sigma(\alpha)^{4^{[F:\mathbb{Q}_q]}}}{\sigma_F(\sigma(\alpha))} \\ &= \frac{\psi(\sigma(\gamma))}{\sigma(\gamma)}.\end{aligned}$$

By comparing this to (5.30) we get that $\xi = \xi'$ and hence $\xi^q = \xi^{\widetilde{M}} = 1$. But since $\widetilde{M}$ and q are coprime we must have $\xi = 1$ which is a contradiction. So our assumption on $\sigma(\gamma)^q$ is false and we get $\sigma(\gamma)^q \notin F(p^{n'-1}M)$. So we can apply Lemma 5.21 and get the following lower bound for the height of $\sigma(\gamma)$

$$\frac{(\log p)^4}{4 \cdot 10^6 p^{32}} \leq h(\sigma(\gamma)) = h(\gamma) \leq (4^{[F:\mathbb{Q}_q]} + 1)h(\alpha).$$

This was the case of $n' \geq 2$. Let us now assume that $n' \leq 1$, which gets us to descent to the tamely ramified case. We do a descent as in the totally ramified case: There is a least integer $n' \leq 1$ such that $\sigma(\gamma) \in F(p^{n'}M)$ for all $\sigma \in \mathrm{Gal}(K(N)/K)$. Lemma 5.26 implies that then also $\gamma \in K(p^{n'}M)$. We will treat this case together with the case $n \leq 1$ where we do not need a descent at all.

Since $h(\sigma(\gamma)) = h(\gamma)$ we can in both cases compute the height of γ where γ will be an element of $K(p^{n'}M)$ where $n' \leq 1$. We want to apply Lemma 5.17, so we will prove that $\gamma \neq 0$ is not a root of unity. Otherwise we would have $4^{[F:\mathbb{Q}_q]}h(\alpha) = h(\alpha^{4^{[F:\mathbb{Q}_q]}}) = h(\gamma\alpha^{4^{[F:\mathbb{Q}_q]}}) = h(\sigma_F(\alpha)) = h(\alpha)$ by the properties of the height and hence $h(\alpha) = 0$. By Kronecker's Theorem this either means $\alpha = 0$ or $\alpha \in \mu_\infty$. But this is a contradiction to our assumption on α. Hence Lemma 5.17 gives

$$h(\gamma) \geq \left(\frac{\log p}{\mathcal{E}(1 + q^{\mathcal{E}})(1 + \frac{1}{2^{10}})}\right)^4.$$

Moreover, we can use inequality (5.28) and $\mathcal{E} \leq \frac{p^4}{2}$ to get

$$
\begin{aligned}
h(\alpha) &\geq \frac{1}{4^{[F:\mathbb{Q}_q]}+1}\left(\frac{\log p}{\mathcal{E}(1+q^{\mathcal{E}})(1+\frac{1}{2^{10}})}\right)^4 \\
&\geq \frac{(\log p)^4}{(4^{[F:\mathbb{Q}_q]}\mathcal{E}q^{\mathcal{E}}2)^4} \\
&\geq \frac{(\log p)^4}{(4^{\frac{p^4}{2}}\frac{p^4}{2}p^{p^4}2)^4} \\
&\geq \frac{(\log p)^4}{4^{2p^4}2p^4p^{2p^4}} \\
&\geq \frac{(\log p)^4}{p^{2p^4\frac{\log 4}{\log p}}2p^4p^{2p^4}} \\
&\geq \frac{(\log p)^4}{2p^{2p^4\frac{\log 4}{\log p}}+4+2p^4} \\
&\geq \frac{(\log p)^4}{p^{4p^4}}.
\end{aligned}
$$

Now we have to put the tamely and totally ramified case into one bound.

We get $h(\alpha) \geq \max(\frac{(\log p)^4}{(4^{[F:\mathbb{Q}_q]}+1)\cdot 2\cdot 10^3 p^{32}}, \frac{1}{4^{[F:\mathbb{Q}_q]}+1}\left(\frac{\log p}{\mathcal{E}(1+q^{\mathcal{E}})(1+\frac{1}{2^{10}})}\right)^4)$. Since

$$
\begin{aligned}
\left(\mathcal{E}(1+q^{\mathcal{E}})(1+\frac{1}{2^{10}})\right)^4 &\geq \left(\frac{p^3}{2}(1+p^{p^3})2\right)^4 \\
&\geq (p^3+p^{p^3+3})^4 \\
&\geq p^{4p^3} \\
&\geq 4\cdot 10^6 p^{32} \qquad \text{for all } p\geq 5.
\end{aligned}
$$

Hence

$$
\begin{aligned}
h(\alpha) &\geq \frac{1}{4^{[F:\mathbb{Q}_q]}+1}\left(\frac{\log p}{\mathcal{E}(1+q^{\mathcal{E}})(1+\frac{1}{2^{10}})}\right)^4 \\
&\geq \frac{(\log p)^4}{(4^{\frac{p^3}{2}}+1)p^{12}(1+p^{p^3})^4} \\
&\geq \frac{(\log p)^4}{p^{4p^4}}.
\end{aligned}
$$

□

Bibliography

[AD00] F. Amoroso and R. Dvornicich. A lower bound for the height in abelian extensions. *J. Number Theory*, 80(2):260–272, 2000.

[ADZ14] Francesco Amoroso, Sinnou David, and Umberto Zannier. On fields with Property (B). *Proc. Amer. Math. Soc.*, 142(6):1893–1910, 2014.

[AZ00] F. Amoroso and U. Zannier. A relative Dobrowolski lower bound over abelian extensions. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 29(3):711–727, 2000.

[AZ10] F. Amoroso and U. Zannier. A uniform relative Dobrowolski's lower bound over abelian extensions. *Bull. Lond. Math. Soc.*, 42(3):489–498, 2010.

[Bak03] Matthew H. Baker. Lower bounds for the canonical height on elliptic curves over abelian extensions. *Int. Math. Res. Not.*, (29):1571–1589, 2003.

[Bil97] Y. Bilu. Limit distribution of small points on algebraic tori. *Duke Math. J.*, 89(3):465–476, 1997.

[BMOR18] M. A. Bennett, G. Martin, K. O'Bryant, and A. Rechnitzer. Explicit bounds for primes in arithmetic progressions. *ArXiv e-prints*, January 2018.

[BS04] Matthew H. Baker and Joseph H. Silverman. A lower bound for the canonical height on abelian varieties over abelian extensions. *Math. Res. Lett.*, 11(2-3):377–396, 2004.

[BZ01] E. Bombieri and U. Zannier. A note on heights in certain infinite extensions of $\mathbf{Q}$. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, 12:5–14 (2002), 2001.

[Che13] S. Checcoli. Fields of algebraic numbers with bounded local degrees and their properties. *Trans. Amer. Math. Soc.*, 365(4):2223–2240, 2013.

[Coh80] H. Cohn. *Advanced number theory*. Dover Publications Inc., New York, 1980. Reprint of ıt A second course in number theory, 1962, Dover Books on Advanced Mathematics.

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[CZ11] Sara Checcoli and Umberto Zannier. On fields of algebraic numbers with bounded local degrees. *C. R. Math. Acad. Sci. Paris*, 349(1-2):11–14, 2011.

[Elk87] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.*, 89(3):561–567, 1987.

[Elk89] N. D. Elkies. Supersingular primes for elliptic curves over real number fields. *Compositio Math.*, 72(2):165–172, 1989.

[FG06] J. Flum and M. Grohe. *Parameterized complexity theory*. Texts in Theoretical Computer Science. An EATCS Series. Springer-Verlag, Berlin, 2006.

[FRM96] E. Fouvry and M. Ram Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.

[Gou89] Edouard Goursat. Sur les substitutions orthogonales et les divisions régulières de l'espace. *Ann. Sci. École Norm. Sup. (3)*, 6:9–102, 1889.

[Hab13] P. Habegger. Small height and infinite nonabelian extensions. *Duke Math. J.*, 162(11):2027–2076, 2013.

[Hua82] L. K. Hua. *Introduction to number theory*. Springer-Verlag, Berlin-New York, 1982. Translated from the Chinese by Peter Shiu.

[Kra83] Kenneth Kramer. A family of semistable elliptic curves with large Tate-Shafarevitch groups. *Proc. Amer. Math. Soc.*, 89(3):379–386, 1983.

[Lan73] S. Lang. *Elliptic functions*. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Amsterdam, 1973. With an appendix by J. Tate.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[LF16] S. Le Fourn. Surjectivity of Galois representations associated with quadratic Q-curves. *Mathematische Annalen*, 365(1):173–214, 2016.

[LMF13] The LMFDB Collaboration. The l-functions and modular forms database. http://www.lmfdb.org, 2013. [Online; accessed 21 March 2014].

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mig89] M. Mignotte. Sur un théorème de M. Langevin. *Acta Arith.*, 54(1):81–86, 1989.

[Neu99] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[RM88] M. Ram Murty. Recent developments in elliptic curves. In *Proceedings of the Ramanujan Centennial International Conference (Annamalainagar, 1987)*, volume 1 of *RMS Publ.*, pages 45–53, Annamalainagar, 1988. Ramanujan Math. Soc.

[RS62] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[Sch73] A. Schinzel. On the product of the conjugates outside the unit circle of an algebraic number. *Acta Arith.*, 24:385–399, 1973. Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday. IV.

[Ser72] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil04] Joseph H. Silverman. A lower bound for the canonical height on elliptic curves over abelian extensions. *J. Number Theory*, 104(2):353–372, 2004.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Smy81] C. J. Smyth. On the measure of totally real algebraic integers. II. *Math. Comp.*, 37(155):205–208, 1981.

[Smy08] Chris Smyth. The Mahler measure of algebraic numbers: a survey. In *Number theory and polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 322–349. Cambridge Univ. Press, Cambridge, 2008.

[vK14] R. von Känel. Integral points on moduli schemes of elliptic curves. *Trans. London Math. Soc.*, 1(1):85–115, 2014.

[vM16] R. von Känel and B. Matschke. Solving S-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via Shimura-Taniyama conjecture, May 2016.

[Vou96] P. Voutier. An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74(1):81–95, 1996.

[Xyl11a] T. Xylouris. On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions. *Acta Arith.*, 150(1):65–91, 2011.

[Xyl11b] T. Xylouris. *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression.* Bonner Mathematische Schriften [Bonn Mathematical Publications], 404. Universität Bonn, Mathematisches Institut, Bonn, 2011. Dissertation for the degree of Doctor of Mathematics and Natural Sciences at the University of Bonn, Bonn, 2011.

Personal information

Last name	Frey, née Raabe
First names	Linda Karina
Address	Friedrichstr. 27 64367 Mühltal, Germany
Phone	+49 178 1968506
E-Mail	Linda.Frey@unibas.ch
Website	www.lorifan.de
Date of birth	23.05.1989
Civil status	Married, two children (*07/2013, *01/2015)

Education and Research Positions

10/2018 to 03/2020 University of Kopenhagen Denmark	early PostDoc.mobility grant (SNF) working on heights, abelian varieties of dimension at least two and their Igusa invariants
04/2015 to 06/2018 Universität Basel Switzerland	PhD in mathematics. Advisor: Prof. Dr. Philipp Habegger Title "Height Lower Bounds in some non-Abelian Extensions"
04/2013 to 03/2015 TU Darmstadt Germany	PhD in mathematics. Advisor: Prof. Dr. Philipp Habegger Working title "Heights and elliptic curves"
09/2012 to 03/2013 Goethe Universität Frankfurt Germany	PhD in mathematics. Advisor: Prof. Dr. Philipp Habegger Working title "Heights and elliptic curves"
09/2011 to 10/2012 ETH Zürich Switzerland	Master of Science ETH in mathematics Master Thesis "Kummer theory on elliptic curves" final grade 5,33 (6: best, 1: worst)
04/2008 to 07/2011 Universität Mainz Germany	Bachelor of Science in mathematics Bachelor Thesis "Freyd-Mitchellscher Einbettungssatz" final grade 2,0 (1: best, 5: worst)

Awards, grants and fellowships

10/2018 to 03/2020 early PostDoc.mobility	Full research stipend of the Swiss National Science Foundation, worth 113.250 CHF
06/2018 Birkhäuser Prize	Award for the best talk in the Swiss Graduate Colloquium 2018
02/2017 to 11/2017 antelope@university	Program of the Universität Basel for highly qualified female PhD students, worth 7.500 CHF (see www.unibas.ch/antelope)
07/2017 to 12/2017 get on track	Liberation of teaching duties, worth 6.000 CHF (see www.unibas.ch/getontrack)
03/2008 Abiturpreis Mathematik	Award of the DMV for an outstanding written exam (highest grade) in the final exams at high school

Teaching activities

09/2015 to date Universität Basel Switzerland	Elliptische Kurven II Seminar for gifted high school students (twice) Lineare Algebra II (twice)
04/2013 to 07/2014 TU Darmstadt Germany	Seminar Kategorientheorie Co-supervised Bachelor's theses
10/2012 to 02/2013 Goethe Universität Frankfurt Germany	Seminar Höhentheorie
09/2011 to 06/2012 ETH Zürich Switzerland	Linear Algebra I Grundlagen der Mathematik II
10/2009 to 08/2011 Universität Mainz Germany	Mathematik für Informatiker I Lineare Algebra I (twice) Lineare Algebra II

Career breaks

08/2016 to 12/2016	Leave (5 months)
08/2015 to 11/2015	Leave (4 months)
08/2014 to 04/2015	Leave (9 months)
06/2013 to 11/2013	Leave (6 months)